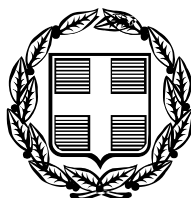


ΕΦΗΜΕΡΙΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ

ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

ΤΕΥΧΟΣ ΔΕΥΤΕΡΟ **Αρ. Φύλλου 1654**

10 Νοεμβρίου 2006

ΑΠΟΦΑΣΕΙΣ

Αριθμ. 2512οικ.

Κύρωση Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου.

ΟΙ ΥΠΟΥΡΓΟΙ ΕΣΩΤΕΡΙΚΩΝ, ΔΗΜΟΣΙΑΣ. ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΑΠΟΚΕΝΤΡΩΣΗΣ - ΜΕΤΑΦΟΡΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

Έχοντας υπόψη:

1) Τις διατάξεις του άρθρου 20 του ν. 3448/2006 «Για την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα και τη ρύθμιση θεμάτων αρμοδιότητας Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης» (ΦΕΚ 57/Α΄),

2) Το Π.Δ. 150/2001 «Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές» (ΦΕΚ 125/Α΄),

3) Την απόφαση της ΕΕΤΤ 248/71/2002 «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής» (ΦΕΚ 603/Β΄),

4) Την υπ’ αριθ. 405/009 /27.9.2006 Απόφαση της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων «Παροχή σύμφωνης γνώμης επί του σχεδίου του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)»,

5) Το γεγονός ότι από την απόφαση αυτή δεν προκαλείται δαπάνη σε βάρος του κρατικού προϋπολογισμού, αποφασίζουμε:

Άρθρο 1

Κυρώνουμε τον Κανονισμό Πιστοποίησης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ), του οποίου το περιεχόμενο έχει ως ακολούθως:

«ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΑΠΟΚΕΝΤΡΩΣΗΣ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΕΦΑΡΜΟΓΗΣ ΠΡΟΓΡΑΜΜΑΤΩΝ ΚΟΙΝΟΤΙΚΟΥ ΠΛΑΙΣΙΟΥ ΣΤΗΡΙΞΗΣ
(ΑΡΧΗ ΠΙΣΤΟΠΟΙΗΣΗΣ ΕΛΛΗΝΙΚΟΥ ΔΗΜΟΣΙΟΥ)
Ηλεκτρονική Διεύθυνση
www.syzefxis.gov.gr

Κανονισμός Πιστοποίησης
της ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΕΛΛΗΝΙΚΟΥ ΔΗΜΟΣΙΟΥ
(ΑΠΕΔ)

1. Εισαγωγή

Η παρούσα πράξη αποτελεί τον Κανονισμό Πιστοποίησης (ΚΠ) της ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ του ΕΛΛΗΝΙΚΟΥ ΔΗΜΟΣΙΟΥ (Πρωτεύουσας Αρχής Πιστοποίησης), σύμφωνα με τις διατάξεις των παραγράφων 1 και 2 του άρθρου 20 του Νόμου 3448/2006 (ΦΕΚ 57/Α), με το οποίο καθορίζονται οι όροι και οι προϋποθέσεις για την παροχή των υπηρεσιών πιστοποίησης από την ΑΠΕΔ ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ) και τις Υποκείμενες Αρχές Πιστοποίησης (ΥπΑΠ), οι οποίες καθορίζονται σύμφωνα με τις διατάξεις της παραγράφου 4 του άρθρου 20 του παραπάνω Νόμου. Επιπλέον, ο παρών Κανονισμός αποτελεί τη Δήλωση Πρακτικής της ΑΠΕΔ, ως Πρωτεύουσας Αρχής Πιστοποίησης για την παροχή υπηρεσιών πιστοποίησης κατά τα προβλεπόμενα στις διατάξεις του Κανονισμού 248/71/2002 της ΕΕΤΤ (ΦΕΚ 603/Β) και του ΠΔ 150/2001 (ΦΕΚ 125/Α) για την εκδοση «αναγνωρισμένων πιστοποιητικών».

Εξάλλου, ο παρών Κανονισμός θέτει τους όρους και τις προϋποθέσεις για την εν γένει παροχή υπηρεσιών πιστοποίησης του Ελληνικού Δημοσίου, μέσω της Υποδομής Δημοσίου Κλειδιού στο πλαίσιο του έργου «ΣΥΖΕΥΞΙΣ», η οποία αναλύεται στα επιμέρους κεφάλαια του παρόντος.

Σε κάθε περίπτωση η ΑΠΕΔ μεριμνά και λαμβάνει τα αναγκαία μέτρα για την εφαρμογή της Πολιτικής Πιστοποίησης, όπως αυτή περιγράφεται στον παρόντα Κανονισμό.

Η υλοποίηση της Υποδομής Δημοσίου Κλειδιού βάσει των διατάξεων του παρόντος διέπεται από την Προκήρυξη, τα τεύχη δημοπράτησης, την απόφαση κατακύρωσης και τη συναφθείσα Σύμβαση στο πλαίσιο του έργου «ΣΥΖΕΥΞΙΣ».

1.1. Περίληψη

Ο παρών ΚΠ εξειδικεύει την Πολιτική Πιστοποίησης της Πρωτεύουσας Αρχής Πιστοποίησης (ΠΑΠ) και των Υποκείμενων Αρχών Πιστοποίησης (ΥπΑΠ) της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) για την έκδοση ψηφιακών πιστοποιητικών τελικών χρηστών. Ειδικότερα, η Πολιτική Πιστοποίησης (ΠΠ) σύμφωνα με τις διατάξεις

ΣΗΜΕΙΩΣΗ: Οι όροι που αναφέρονται με Κεφαλαίο αρχικό γράμμα στον παρόντα ΚΠ αποτελούν βασικούς όρους. Στο Παράρτημα του παρόντος υπάρχει πλήρης κατάλογος.

του παρόντος, καθορίζει τους όρους, τις προϋποθέσεις καθώς και τις τεχνικές προδιαγραφές για την έγκριση, έκδοση, χειρισμό, χρήση, ανάκληση και ανανέωση των παραπάνω ψηφιακών πιστοποιητικών και την παροχή των σχετικών υπηρεσιών πιστοποίησης.

Ειδικότερα: ο παρών ΚΠ περιγράφει:

Τις υποχρεώσεις των Υποκείμενων Αρχών Πιστοποίησης (Certification Authorities), των Αρχών Εγγραφής (Registration Authorities), των Τελικών Χρηστών και των Τρίτων Συμμετεχόντων.

Τα θέματα που καλύπτονται στους Όρους Χορήγησης Πιστοποιητικών Τελικού Χρήστη (ΟΧΠ) και τους Όρους Τρίτων Συμμετεχόντων (ΟΤΣ).

Τις μεθόδους που χρησιμοποιούνται για την επιβεβαίωση της ταυτότητας των Τελικών Χρηστών.

Τις λειτουργικές διαδικασίες ως προς τις υπηρεσίες κύκλου ζωής Πιστοποιητικού: υποβολή αιτήματος για Πιστοποιητικά, έκδοση, αποδοχή, ανάκληση και ανανέωση Πιστοποιητικού.

Το περιεχόμενο των Πιστοποιητικών και των Καταλόγων Ανακληθέντων Πιστοποιητικών (ΚΑΠ).

Τις λειτουργικές διαδικασίες ασφάλειας ως προς την καταγραφή στοιχείων ελέγχου, την τήρηση αρχείων και την αποκατάσταση καταστροφών.

Τους κανονισμούς φυσικής ασφάλειας, ασφάλειας προσωπικού, διαχείρισης κλειδιών και λογικής ασφάλειας.

Τη διαχείριση του ΚΠ, συμπεριλαμβανομένων των μεθόδων τροποποίησής του.

Στον παρακάτω πίνακα 1 περιλαμβάνεται κατάλογος των προς δημοσίευση εγγράφων της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ), καθώς και τις τοποθεσίες δημοσίευσής τους. Τα έγγραφα που δε διατίθενται προς δημοσίευση αποτελούν εμπιστευτικό υλικό της ΑΠΕΔ.

Πίνακας 1 -– Διαθέσιμα Έγγραφα Κανονισμών

Έγγραφα	Κατάσταση	Τοποθεσία Δημοσίευσης για το Κοινό
Κανονισμός Πιστοποίησης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)	Δημόσιο	Χώρος Αποθήκευσης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) σύμφωνα με την § 2.6 του ΚΠ Βλ. http://www.syzefxis.gov.gr
Όροι Χορήγησης Πιστοποιητικών Τελικών Χρηστών (ΟΧΠ) και Όροι Τρίτου Συμμετέχοντα (ΟΤΣ)	Δημόσιο	Χώρος Αποθήκευσης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) σύμφωνα με την § 2.6 του ΚΠ Βλ. http://www.syzefxis.gov.gr

1.2. Συμμόρφωση με τα Ισχύοντα Κριτήρια

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) έχει προσαρμόσει τον παρόντα ΚΠ στο Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (Πλαίσιο Πολιτικής Πιστοποιητικού Υποδομής Δημόσιου Κλειδιού και Κανονισμών Πιστοποίησης X.509 για το Διαδίκτυο), γνωστό και ως RFC 2527, του Internet Engineering Task Force, φορέας ο οποίος είναι υπεύθυνος για τον καθορισμό προτύπων στο Διαδίκτυο, για να διευκολύνει την απεικόνιση της εφαρμοζόμενης πολιτικής πιστοποίησης. Μικρές αποκλίσεις από την δομή του RFC 2527 σε επιμέρους λεπτομέρειες, είναι απαραίτητες εξαιτίας της πολυπλοκότητας του λειτουργικού μοντέλου της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ). Η ΑΠΕΔ, εξάλλου, διατηρεί το δικαίωμα να προβαίνει στις απαραίτητες ενέργειες στο πλαίσιο του παρόντος Κανονισμού, όπου αυτό κρίνεται σκόπιμο, με σκοπό τη βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών της.

1.2.1. Πολιτική Πιστοποίησης

1.2.1.1. Πολιτική Πιστοποίησης 1 (ΠΠ1)

Η Πολιτική Πιστοποίησης 1 (ΠΠ 1) αναφέρεται σε Αναγνωρισμένα Πιστοποιητικά τελικών χρηστών. Τα πιστοποιητικά που εκδίδονται βάσει της ΠΠ 1 χρησιμοποιούνται για ψηφιακή υπογραφή (προηγμένη ηλεκτρονική υπογραφή) ηλεκτρονικών μηνυμάτων ή εγγράφων. Ήτοι, τα πιστοποιητικά που εκδίδονται βάσει της ΠΠ 1 είναι κατάλληλα για να υποστηρίξουν προηγμένη ηλεκτρονική υπογραφή, σύμφωνα με τις διατάξεις της παραγρ. 1 του άρθρου 3 του ΠΔ 150/2001 (ΦΕΚ 125/Α), η οποία βασίζεται σε αναγνωρισμένο πιστοποιητικό και δημιουργείται από ασφαλή διάταξη δημιουργίας υπογραφής, οπότε και επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο, με την επιφύλαξη της παραγράφου 2 του άρθρου 1 του ιδίου ΠΔ. Η ΠΠ 1 αντιστοιχεί στην δημόσια πολιτική πιστοποιητικών "QCP + SSCD" όπως περιγράφεται στο «έγγραφο Πολιτικής ETSI 101 456». Ως «έγγραφο Πολιτικής ETSI 101 456» ορίζεται το "ETSI Policy Document" δηλαδή η Τεχνική Προδιαγραφή του European Telecommunications Standards Institute ("ETSI") 101 456 αναφορικά με τις Απαιτήσεις Πολιτικής για Αρχές Πιστοποίησης που εκδίδουν Αναγνωρισμένα Πιστοποιητικά.

Τα Πιστοποιητικά που εκδίδονται με βάση την ΠΠ 1 πιστοποιούν την αντιστοιχία του φυσικού προσώπου (τελικού χρήστη) με τα στοιχεία που αναφέρονται στην ταυτότητά του (ταυτοποίηση).

Η ταυτοποίηση των Τελικών Χρηστών προϋποθέτει τη φυσική παρουσία τους ενώπιον αντιπροσώπων της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (υπάλληλοι των Εντεταλμένων Γραφείων), οι οποίοι ελέγχουν τα έγγραφα που τεκμηριώνουν την ταυτότητα του Τελικού Χρήστη (ΚΠ § 2.1.3).

Τα Αναγνωρισμένα Πιστοποιητικά Τελικών Χρηστών αναφέρονται αποκλειστικά και μόνο σε φυσικά πρόσωπα. Σε κάθε περίπτωση το Αναγνωρισμένο Πιστοποιητικό συνδέεται κατ' αποκλειστικότητα με το φυσικό πρόσωπο που ασκεί συγκεκριμένη αρμοδιότητα στο πλαίσιο άσκησης των καθηκόντων του και στη συγκεκριμένη οργανική μονάδα που υπηρετεί.

1.2.1.2. Πολιτική Πιστοποίησης 2 (ΠΠ2)

Η Πολιτική Πιστοποίησης 2 (ΠΠ 2) αναφέρεται σε πιστοποιητικά τελικών χρηστών που χρησιμοποιούνται για κρυπτογράφηση ηλεκτρονικών μηνυμάτων ή εγγράφων.

1.2.2. Κριτήρια ένταξης ΥπΑΠ στην παρούσα Υποδομή Δημοσίου Κλειδιού

Ως ΥπΑΠ στην παρούσα Υποδομή Δημοσίου Κλειδιού, σύμφωνα με τις διατάξεις του παρόντος, εντάσσονται οι φορείς του δημόσιου τομέα οι οποίοι ασκούν αρμοδιότητες για τη διεκπεραίωση των οποίων απαιτείται

υψηλό επίπεδο ασφαλείας κάνοντας χρήση υπηρεσιών πιστοποίησης, όπως ιδίως για τη διακίνηση αποφάσεων, πιστοποιητικών και βεβαιώσεων ή εγγράφων που συνδέονται με την παραγωγή εννόμων αποτελεσμάτων ή σχέσεων ή με την άσκηση δικαιώματος.

1.2.3. Προσφερόμενες Υπηρεσίες της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) παρέχει υπηρεσίες πιστοποίησης σε τελικούς χρήστες των Φορέων του δημόσιου τομέα που εντάσσονται στην παρούσα Υποδομή Δημοσίου Κλειδιού.

1.3. Τιμές Προσδιοριστή Αντικειμένου

Τα πιστοποιητικά της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δύναται να περιλάβουν τιμές προσδιοριστή αντικειμένου (Object Identifier) που αντιστοιχούν στην εκάστοτε πολιτική πιστοποιητικού που ακολουθείται. Η τιμή προσδιοριστή αντικειμένου για την:

ο ΠΠ 1 είναι: [όπως θα οριστεί από τον ΕΛΟΤ]

ο ΠΠ 2 είναι: [όπως θα οριστεί από τον ΕΛΟΤ]

1.4. Πεδίο Εφαρμογής ΚΠ

Ο παρών ΚΠ διέπει τις υπηρεσίες Υποδομής Δημοσίου Κλειδιού που παρέχονται από φορείς του Δημόσιου Τομέα.

1.4.1. Σχέση Πρωτεύουσας Αρχής Πιστοποίησης με Υποκείμενες Αρχές Πιστοποίησης

Η Πρωτεύουσα Αρχή Πιστοποίησης είναι αρμόδια για την πιστοποίηση, τον καθορισμό των κατευθύνσεων και το συντονισμό των άλλων δημοσίων υπηρεσιών ή φορέων του δημόσιου τομέα (Υποκείμενες Αρχές Πιστοποίησης), οι οποίοι διαχειρίζονται ψηφιακά πιστοποιητικά και εντάσσονται στην παρούσα Υποδομή Δημοσίου Κλειδιού, κατά τα οριζόμενα στην παράγραφο 2 του άρθρου 20 του Ν 3448/2006 (ΦΕΚ 57/Α) και εγγράφεται στο μητρώο Παρόχων Υπηρεσιών Πιστοποίησης της ΕΕΤΤ, σύμφωνα με το άρθρο 10 του υπ' αριθ. 248/71/2002 Κανονισμού της ΕΕΤΤ (ΦΕΚ 603 Β).

Ως εκ τούτου, 1) Η ΑΡΧΗ ΠΙΣΤΟΠΟΙΗΣΗΣ ΕΛΛΗΝΙΚΟΥ ΔΗΜΟΣΙΟΥ (ΑΠΕΔ) η οποία ενεργεί ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ), πιστοποιεί τις Υποκείμενες Αρχές Πιστοποίησης με την έκδοση αντίστοιχων πιστοποιητικών και εν συνεχεία,

2) οι Υποκείμενες Αρχές Πιστοποίησης (ΥπΑΠ), εφόσον ενταχθούν στην Υποδομή Δημοσίου Κλειδιού, βάσει των διατάξεων του παρόντος και πιστοποιηθούν από την ΑΠΕΔ, σύμφωνα με τα παραπάνω, διαχειρίζονται τα πιστοποιητικά τελικών χρηστών σύμφωνα με την ΠΠ1 και ΠΠ2 του παρόντος και ορίζουν μια ή περισσότερες οργανικές μονάδες οι οποίες, αφού γνωστοποιηθούν στην ΑΠΕΔ, θα ασκήσουν τις αρμοδιότητες των «Αρχών Εγγραφής» και των «Εντεταλμένων Γραφείων » (ΚΠ § 1.4.2 και ΚΠ § 1.4.2.1)

Ειδικότερα, οι Υποκείμενες Αρχές Πιστοποίησης (ΥπΑΠ) αναλαμβάνουν τη διαχείριση του κύκλου ζωής των ψηφιακών πιστοποιητικών τελικών χρηστών (έκδοση-ανάκληση-ανανέωση-ανάκτηση κλπ.).

Μέχρι την εγγραφή τους στο μητρώο της ΕΕΤΤ, κατά τις κείμενες διατάξεις, όπως ιδίως τον υπ΄ αριθμ. 248/71/2002 Κανονισμό της ΕΕΤΤ (ΦΕΚ 603/Β΄), οι ΥπΑΠ παρέχουν υπηρεσίες πιστοποίησης ως εντεταλμένα όργανα της ΑΠΕΔ.

1.4.2. Αρχές Εγγραφής

Οι Αρχές Εγγραφής (ΑΕ) προκειμένου για τη χορήγηση των ψηφιακών πιστοποιητικών σύμφωνα με τις διατάξεις του παρόντος, είναι αρμόδιες για την έγκριση των ηλεκτρονικών εγγραφών των τελικών χρηστών, διαδικασία κατά την οποία υποβάλλονται ηλεκτρονικά από τους τελικούς χρήστες τα στοιχεία ταυτότητάς τους, εφόσον τα εν λόγω στοιχεία έχουν βεβαιωθεί (επαληθευτεί) αρμοδίως από τους υπαλλήλους των Εντεταλμένων Γραφείων που υπάγονται στις παραπάνω ΑΕ. Επιπλέον, οι ΑΕ εγκρίνουν κατά τον ίδιο τρόπο, την ανάκληση/ανάκτηση ή ανανέωση Πιστοποιητικών.

1.4.2.1. Εντεταλμένα Γραφεία

Κάθε Αρχή Εγγραφής εποπτεύει έναν αριθμό Εντεταλμένων Γραφείων. Τα Εντεταλμένα Γραφεία είναι αρμόδια για την επιβεβαίωση - επαλήθευση των στοιχείων ταυτότητας των Τελικών Χρηστών καθώς και την διοικητική διεκπεραίωση των αιτημάτων για έκδοση/ανανέωση/ανάκληση και ανάκτηση πιστοποιητικών Τελικών Χρηστών και αναφέρονται στην προϊσταμένη Αρχή Εγγραφής.

1.4.3. Τελικοί Χρήστες

Ως Τελικοί Χρήστες νοούνται τα φυσικά πρόσωπα, κάτοχοι πιστοποιητικών σύμφωνα με τις διατάξεις του παρόντος που έχουν συγκεκριμένη αρμοδιότητα στο πλαίσιο άσκησης των καθηκόντων τους και στη συγκεκριμένη οργανική μονάδα στην οποία υπηρετούν. Η επιλογή των τελικών χρηστών γίνεται από τις ΥπΑΠ με στόχο την εξυπηρέτηση αναγκών του οικείου φορέα οι οποίες είναι σύμφωνες με την εφαρμογή/χρήση των ψηφιακών πιστοποιητικών όπως περιγράφονται στον παρόντα ΚΠ.

1.4.4. Εφαρμογή των Πιστοποιητικών

Οι προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε πιστοποιητικά που ακολουθούν την ΠΠ 1 και έχουν δημιουργηθεί από ασφαλή διάταξη δημιουργίας υπογραφής επέχουν θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο όπως αναφέρεται στην κείμενη εθνική νομοθεσία (ΠΔ 150/2001), με την επιφύλαξη της παραγράφου 2 του άρθρου 1 του παραπάνω ΠΔ.

Τα πιστοποιητικά Τελικών Χρηστών που προβλέπονται στην παρούσα Υποδομή Δημοσίου Κλειδιού εκδίδονται σε φυσικά πρόσωπα, είναι αυστηρώς προσωπικά και χρησιμοποιούνται στο πλαίσιο της άσκησης των καθηκόντων των Τελικών Χρηστών για την εξυπηρέτηση αναγκών του φορέα.

Οι εφαρμογές στις οποίες μπορούν να χρησιμοποιηθούν τα πιστοποιητικά τελικών χρηστών που θα παρασχεθούν βάσει της Υποδομής Δημοσίου Κλειδιού του παρόντος και με την χρήση προηγμένης ηλεκτρονικής υπογραφής, όπου απαιτείται, είναι:

- Ασφαλής χρήση ηλεκτρονικού ταχυδρομείου / μηνυμάτων (υπογραφή και κρυπτογράφηση)
- Υπογραφή και κρυπτογράφηση ηλεκτρονικών αρχείων (π.χ. αρχεία Adobe Acrobat)
- Ασφαλής προσδιορισμός ηλεκτρονικής ταυτότητας
- Έλεγχος πρόσβασης
- Προσδιορισμός του Υπευθύνου για κάθε σχετική ηλεκτρονική επικοινωνία / συναλλαγή

Μελλοντικές χρήσεις πιστοποιητικών τελικών χρηστών

Μελλοντικές χρήσεις εφαρμογών πιστοποιητικών τελικών χρηστών επιτρέπονται κατόπιν εγκρίσεως της ΑΠΕΔ.

Περιορισμοί στη χρήση των πιστοποιητικών

Τα πιστοποιητικά της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) αν και αποτελούν Πιστοποιητικά για γενική χρήση, έχουν περιορισμούς στη χρήση τους όπως ορίζεται στη παράγραφο 7 του παρόντος. Σε κάθε περίπτωση οι διατάξεις του παρόντος δεν θίγουν διατάξεις που αναφορικά με τη σύναψη και την ισχύ συμβάσεων ή εν γένει τη σύσταση νομικών υποχρεώσεων, επιβάλλουν τη χρήση ορισμένου τύπου, ούτε διατάξεις για την αποδεικτική ή άλλη χρήση εγγράφων ή διατάξεις με τις οποίες απαγορεύεται να διακινούνται και να καθίστανται γνωστά έγγραφα ορισμένων κατηγοριών και δεδομένα προσωπικού χαρακτήρα, σύμφωνα και με τις διατάξεις της παρ. 2 του άρθρου 1 του ΠΔ 150/2001 (ΦΕΚ 25/Α) .

Απαγορευμένες Εφαρμογές

Τα Πιστοποιητικά δεν έχουν σχεδιαστεί, δεν αποσκοπούν και δεν είναι εγκεκριμένα να χρησιμοποιηθούν σε περιπτώσεις όπου απαιτείται τήρηση στοιχείων υψηλής διαβάθμισης ή συνθηκών υψηλής ασφάλειας (απόρρητο, διακίνηση διαβαθμισμένων στοιχείων ή εγγράφων). Εξάλλου, απαγορεύεται η χρήση των πιστοποιητικών για σκοπούς άλλους από εκείνους για τους οποίους αυστηρά εκδόθηκαν.

1.5. Στοιχεία Επικοινωνίας

1.5.1. Έκδοση Κανονισμού Πιστοποίησης (ΚΠ)

Τον παρόντα ΚΠ εκδίδει και τροποποιεί η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ), ως Πρωτεύουσα Αρχή Πιστοποίησης σύμφωνα με τις διατάξεις της παραγράφου 2 του άρθρου 1 του Ν 3448/2006 (ΦΕΚ 57/Α). Τυχόν αιτήματα για διευκρινίσεις επί των κεφαλαίων του παρόντος θα απευθύνονται προς την ΑΠΕΔ.

2. Γενικές Διατάξεις

2.1. Αρμοδιότητες και υποχρεώσεις εμπλεκομένων

2.1.1. Αρμοδιότητες ΥπΑΠ

Οι ΥπΑΠ εκπληρώνουν τις υποχρεώσεις που αναφέρονται στον παρόντα ΚΠ σύμφωνα με το Π.Δ. 150/2001 (ΦΕΚ 125/Α), τον Κανονισμό 248/71/2002 της ΕΕΤΤ (ΦΕΚ 603/Β΄) και το έγγραφο "Πολιτικής ETSI 101 456".

Οι ΥπΑΠ που εντάσσονται στην Υποδομή Δημοσίου Κλειδιού, βάσει του παρόντος, καθορίζουν και γνωστοποιούν υποχρεωτικά στην ΑΠΕΔ τις υπαγόμενες σε αυτές οργανικές μονάδες, οι οποίες ασκούν τις αρμοδιότητες των Αρχών Εγγραφής και των Εντεταλμένων Γραφείων και διαχειρίζονται τα πιστοποιητικά που εκδίδονται βάσει της ΠΠ1 και ΠΠ2 του παρόντος.

Ειδικότερα οι ΥπΑΠ διαχειρίζονται τα πιστοποιητικά Τελικών Χρηστών της ΑΠΕΔ και προβαίνουν στις παρακάτω ενέργειες:

1) Ελέγχουν και αποδέχονται τις Ηλεκτρονικές Εγγραφές για πιστοποιητικά από τους Τελικούς Χρήστες σύμφωνα με τις διαδικασίες που περιγράφονται στον παρόντα Κανονισμό Πιστοποίησης (ΚΠ § 4.1.1) και διενεργούν την έκδοση, ανανέωση, ανάκτηση ή ανάκληση του πιστοποιητικού, ανάλογα με το αίτημα.

2) Εκδίδουν και δημοσιεύουν Κατάλογο Ανακληθέντων Πιστοποιητικών.

Ειδικότερα η κάθε ΥπΑΠ:

1. Δέχεται αιτήσεις έκδοσης, ανάκλησης πιστοποιητικών ή/και ανάκτησης πιστοποιητικών κρυπτογράφησης σύμφωνα με τις διαδικασίες που περιγράφονται στον παρόντα ΚΠ.

2. Επαληθεύει την ταυτότητα των τελικών χρηστών που αιτούνται την ανάκληση πιστοποιητικών ή/και την ανάκτηση πιστοποιητικών κρυπτογράφησης.

3. Εκδίδει και δημοσιεύει Κατάλογο Ανακληθέντων Πιστοποιητικών (ΚΑΠ-CRL).

2.1.1.1. Προστασία του ιδιωτικού κλειδιού της ΥπΑΠ

1. Το ιδιωτικό κλειδί κάθε ΥπΑΠ προστατεύεται μέσω αξιόπιστων προϊόντων ηλεκτρονικής υπογραφής, όπως αυτά ορίζονται σύμφωνα με το άρθρο 2, στοιχείο 12 του ΠΔ 150/2001 και τον παρόντα ΚΠ.

2. Πρέπει να ακολουθούνται οι περιορισμοί χρήσης του ιδιωτικού κλειδιού της ΥπΑΠ, όπως ορίζονται στον παρόντα Κανονισμό.

Τα ιδιωτικά κλειδιά των ΥπΑΠ μπορεί να χρησιμοποιηθούν μόνο για την υπογραφή πιστοποιητικών Τελικών Χρηστών και των αντίστοιχων Καταλόγων Ανάκλησης Πιστοποιητικών (ΚΑΠ -CRL).

2.1.2. Αρμοδιότητες Αρχών Εγγραφής

Οι Αρχές Εγγραφής είναι αρμόδιες για την άσκηση των καθηκόντων ταυτοποίησης, αποδοχής ή απόρριψης Ηλεκτρονικών Εγγραφών για Πιστοποιητικά και την αποδοχή ή απόρριψη αιτημάτων ανάκλησης, ανάκτησης ή ανανέωσης Πιστοποιητικού. Στις αρμοδιότητες αυτές περιλαμβάνονται και οι ενέργειες που επιτελούνται από τα Εντεταλμένα Γραφεία.

Οι παραπάνω αρμοδιότητες περιλαμβάνουν:

1. Την επαλήθευση της ταυτότητας του τελικού χρήστη που θα πιστοποιηθεί σύμφωνα με τις διαδικασίες που προβλέπονται στον παρόντα ΚΠ (βλ. § 3.1.7).

2. Την επαλήθευση ότι ο ενδιαφερόμενος Τελικός Χρήστης έχει στην κατοχή του το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που περιλαμβάνεται στην Ηλεκτρονική Εγγραφή για πιστοποιητικά, σύμφωνα με τις διαδικασίες που προβλέπονται στον παρόντα ΚΠ.

3. Την αποθήκευση των αποδεικτικών στοιχείων και των «Εντύπων ΥΔΚ», πέραν του χρονικού διαστήματος ισχύος του πιστοποιητικού, σύμφωνα με τον παρόντα ΚΠ και τις εκάστοτε ισχύουσες διατάξεις.

4. Ο Υπεύθυνος της Αρχής Εγγραφής έχει την υποχρέωση να προστατεύει το ζεύγος κλειδιών του «Υπευθύνου Αρχής Εγγραφής», σύμφωνα με τον παρόντα ΚΠ.

5. Ο Υπεύθυνος της Αρχής Εγγραφής έχει την υποχρέωση να χρησιμοποιεί το ιδιωτικό κλειδί «Υπευθύνου Αρχής Εγγραφής» για την αποδοχή Ηλεκτρονικών Εγγραφών για πιστοποιητικά (αναγνωρισμένα ή μη) ή για την διεκπεραίωση αιτημάτων ανάκλησης/ανανέωσης/ανάκτησης πιστοποιητικών και δεν μπορεί να το χρησιμοποιεί για σκοπούς άλλους από αυτούς για τους οποίους του έχει χορηγηθεί.

Σύμφωνα με τον παρόντα ΚΠ, κάθε ΥπΑΠ φέρει το σύνολο των υποχρεώσεων που αναφέρονται για τις Αρχές Εγγραφής και τα Εντεταλμένα Γραφεία.

2.1.3. Υποχρεώσεις Εντεταλμένων Γραφείων

Οι υποχρεώσεις των Εντεταλμένων Γραφείων εξειδικεύονται παρακάτω για τους Υπεύθυνους και τους Υπαλλήλους των Εντεταλμένων Γραφείων.

Οι Υπεύθυνοι των Εντεταλμένων Γραφείων:

1. Παραλαμβάνουν τον απαιτούμενο αριθμό φακέλων όπου περιλαμβάνονται οι μυστικοί αριθμοί πρόσβασης στην έξυπνη κάρτα (PIN-PUK / Personal Identification Number- Personal Unblocking Key) και φροντίζουν για την ασφαλή φύλαξη τους.

2. Ελέγχουν την διαδικασία επιβεβαίωσης της ταυτότητας του τελικού χρήστη που έχει διενεργηθεί από τους Υπαλλήλους των Εντεταλμένων Γραφείων.

3. Αποστέλλουν στους Υπευθύνους των Αρχών Εγγραφής, μέσω υπογεγραμμένου μηνύματος ηλεκτρονικού ταχυδρομείου, τα πλήρη στοιχεία των τελικών χρηστών που προσήλθαν στο Εντεταλμένο Γραφείο και υπέγραψαν το "Έντυπο ΥΔΚ" ανάλογα με τον επιδιωκόμενο σκοπό (π.χ. για την έκδοση νέων πιστοποιητικών, ανάκληση ή ανανέωση πιστοποιητικών ή ανάκτηση πιστοποιητικού κρυπτογράφησης).

Οι Υπάλληλοι των Εντεταλμένων Γραφείων:

1. Επιβεβαιώνουν την ταυτότητα των τελικών χρηστών που παρουσιάζονται αυτοπροσώπως στο Εντεταλμένο Γραφείο (βλ. § 3.1.7).

2. Επιβεβαιώνουν τα στοιχεία του «Εντύπου ΥΔΚ» που υποβάλλεται από τον Τελικό Χρήστη.

3. Παραδίδουν στον Τελικό Χρήστη τον σφραγισμένο φάκελο που περιλαμβάνει τους μυστικούς αριθμούς πρόσβασης στην έξυπνη κάρτα (PIN-PUK/ Personal Identification Number - Personal Unblocking Key), εάν απαιτείται, εφόσον έχουν αντιστοιχήσει τον σειριακό αριθμό του φακέλου με τον αντίστοιχο της έξυπνης κάρτας του τελικού χρήστη.

2.1.4. Υποχρεώσεις Τελικού Χρήστη

Οι υποχρεώσεις Τελικού Χρήστη ισχύουν βάσει του παρόντος ΚΠ, μέσω των Όρων Χορήγησης Πιστοποιητικού που εγκρίνονται από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ). Οι ισχύοντες ΟΧΠ δημοσιεύονται στη διεύθυνση http://www.syzefxis.gov.gr.

Κάθε Τελικός Χρήστης, πριν υποβάλει Ηλεκτρονική Εγγραφή για πιστοποιητικά (υπογραφής -κρυπτογράφησης), παραλαμβάνει αυτοπροσώπως (προσκομίζοντας τα απαιτούμενα έγγραφα ταυτοποίησης, σύμφωνα με την § 3.1.7):

- την έξυπνη κάρτα και το "Έντυπο ΥΔΚ" από τον Προϊστάμενο της Δημόσιας Διοικητικής Αρχής στην οποία υπάγεται
- τον αντίστοιχο προς την έξυπνη κάρτα σφραγισμένο φάκελο όπου περιλαμβάνονται οι μυστικοί αριθμοί πρόσβασης σε αυτή (PIN-PUK) από το αρμόδιο Εντεταλμένο Γραφείο εφόσον έχει υποβληθεί το "Έντυπο ΥΔΚ"

Οι Όροι Χορήγησης Πιστοποιητικού γνωστοποιούνται στους Τελικούς Χρήστες - υπαλλήλους πριν αυτοί υποβάλουν τις απαιτούμενες πληροφορίες εγγραφής ("Έντυπο ΥΔΚ") και περιλαμβάνουν τα ακόλουθα:

Ο Τελικός Χρήστης:

1. Αναγνωρίζει και συμφωνεί ότι η διαδικασία υποβολής Ηλεκτρονικής Εγγραφής για ψηφιακά πιστοποιητικά υπογραφής και κρυπτογράφησης καθώς και κάθε ενέργεια που σχετίζεται με την υποδομή δημοσίου κλειδιού της ΑΠΕΔ, διέπεται από τον Κανονισμό Πιστοποίησης ('ΚΠ') της ΑΠΕΔ, όπως εκάστοτε ισχύει, ο οποίος ενσωματώνεται κατά παραπομπή στους παρόντες Όρους. Ο ΚΠ δημοσιεύεται στο διαδίκτυο, στο Χώρο Αποθήκευσης της ΑΠΕΔ, στην ηλεκτρονική διεύθυνση http://www.syzefxis.gov.gr. Οι τροποποιήσεις του ΚΠ επίσης, ανακοινώνονται στο Χώρο Αποθήκευσης της ΑΠΕΔ στην ηλεκτρονική διεύθυνση http://www.syzefxis.gov.gr.

2. Η έξυπνη κάρτα ή το usb token που έχει παραλάβει αποτελεί Ασφαλή Διάταξη Δημιουργίας Υπογραφής σύμφωνα με τις απαιτήσεις που παρατίθενται στο Παράρτημα ΙΙΙ του ΠΔ 150/2001 (ΦΕΚ 125/Α). Αυτό σημαίνει πως απαιτείται η χρήση αυτής της συσκευής και μόνο για τα ψηφιακά πιστοποιητικά που θα δημιουργηθούν. Ειδικά για την έξυπνη κάρτα, θα πρέπει μόλις παραληφθεί να υπογραφεί στο ειδικό πλαίσιο στην πίσω πλευρά.

3. Η έξυπνη κάρτα, οι αντίστοιχοι κωδικοί PIN-PUK, καθώς και τα ψηφιακά πιστοποιητικά που θα παραχθούν σε αυτή είναι αυστηρά προσωπικά και ο Τελικός Χρήστης είναι ο μόνος αρμόδιος για τη χρήση τους. Όλα τα παραπάνω θα πρέπει να αντιμετωπίζονται όπως κάθε αντικείμενο που περιλαμβάνει προσωπικά δεδομένα (π.χ. μια πιστωτική κάρτα).

4. Δεν θα πρέπει να διατηρεί στον ίδιο χώρο την έξυπνη κάρτα και τους προσωπικούς του αριθμούς PIN-PUK. Σε καμία περίπτωση δεν πρέπει να αφήνει εκτεθειμένη την έξυπνη κάρτα του σε οποιοδήποτε μέρος. Αυτό ισχύει ακόμα και για το χώρο εργασίας του. Επίσης, μετά τη χρήση της θα πρέπει να την αποθηκεύει σε ασφαλές μέρος.

5. Δεν θα πρέπει να δανείζει την έξυπνη κάρτα ή να γνωστοποιεί τους κωδικούς αριθμούς PIN-PUK σε οποιονδήποτε, ακόμα και εάν είναι συνάδελφός του, υπεύθυνος του Φορέα στον οποίο εργάζεται, προϊστάμενος ή υπεύθυνος του Εντεταλμένου Γραφείου από όπου παρέλαβε τους κωδικούς αριθμούς PIN-PUK.

6. Το ψηφιακό του Πιστοποιητικό Υπογραφής (ΠΠ 1 στον ΚΠ) θα εκδοθεί σύμφωνα με τις απαιτήσεις που παρατίθενται στο ΠΔ 150/2001 (ΦΕΚ 125/Α). Ο προσδιοριστής αντικειμένου (Object IDentifier ή 'OID') που αντιστοιχεί στο ψηφιακό πιστοποιητικό Υπογραφής είναι το: id-edsp-dl2 (2.16.840.1.113733.1.7.44.2) (QCP public+SSCD σύμφωνα με το πρότυπο "ETSI 101 456").

7. Οι πληροφορίες που περιλαμβάνονται στην Ηλεκτρονική Εγγραφή για Πιστοποιητικά, καθώς και τα λοιπά στοιχεία που παρέχονται από τον Τελικό Χρήστη είναι αληθή και πλήρη σύμφωνα με τις απαιτήσεις του ΚΠ.

8. Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται αποκλειστικά για εγκεκριμένους και σύννομους σκοπούς, σύμφωνα με τον ΚΠ. Κανένα μη-εξουσιοδοτημένο πρόσωπο δεν πρέπει να έχει πρόσβαση στο ιδιωτικό κλειδί του πιστοποιητικού Υπογραφής (ΠΠ 1). Ο Τελικός Χρήστης θα πρέπει να επιδείξει λογική μέριμνα για να αποφευχθεί η μη-εξουσιοδοτημένη χρήση των ιδιωτικών του κλειδιών. Επίσης θα πρέπει να παύσει άμεσα την χρήση των ιδιωτικών κλειδιών του μετά την ημερομηνία λήξεως τους και απαγορεύεται απολύτως να επέμβει στο σχεδιασμό της τεχνικής εφαρμογής της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ).

9. Θα πρέπει να ακολουθεί τους Όρους Τρίτους Συμμετέχοντα (ΟΤΣ) της ΑΠΕΔ όταν βασίζεται σε οποιαδήποτε ψηφιακό πιστοποιητικό που έχει εκδοθεί από την ΑΠΕΔ ή από ΥπΑΠ. Οι ΟΤΣ δημοσιεύονται στο χώρο αποθήκευσης της ΑΠΕΔ στη διεύθυνση : http://www.syzefxis.gov.gr.

10. Θα πρέπει να ενημερώσει άμεσα την ΑΠΕΔ ή τις ΥπΑΠ (μέσω των αρμόδιων Εντεταλμένων Γραφείων) χωρίς καμία λογική καθυστέρηση, εφόσον: α) έχει υπόνοιες πως έχει παραβιαστεί, χαθεί, κλαπεί ή πιθανώς εκτεθεί σε κίνδυνο κάποιο ιδιωτικό του κλειδί , β) έχουν εκτεθεί σε κίνδυνο τα δεδομένα ενεργοποίησης της έξυπνης κάρτας του (π.χ. κωδικός PIN) , γ) υπάρχει απώλεια, κλοπή ή καταστροφή της έξυπνης κάρτας και/ή

δ) υπάρχουν ανακρίβειες ή μεταβολές στο περιεχόμενο των πιστοποιητικών του.

11. Θα πρέπει να επαληθεύσει την εγκυρότητα, αναστολή ή ανάκληση ενός πιστοποιητικού που έχει εκδοθεί από την ΑΠΕΔ χρησιμοποιώντας τις τρέχουσες πληροφορίες καταλόγου ανάκλησης πιστοποιητικού (ΚΑΠ).

12. Θα πρέπει να χρησιμοποιήσει το ψηφιακό πιστοποιητικό Υπογραφής (ΠΠ 1 στον ΚΠ) για τη δημιουργία ηλεκτρονικών υπογραφών και μόνο. Επισημαίνεται ότι το ιδιωτικό κλειδί του ψηφιακού πιστοποιητικού Κρυπτογράφησης (ΠΠ 2 στον ΚΠ) έχει παραχθεί για λογαριασμό του κεντρικοποιημένα από την ΑΠΕΔ και συνεπώς έχει δημιουργηθεί αντίγραφο ασφαλείας του με σκοπό να υπάρχει δυνατότητα ανάκτησής του στην περίπτωση που χάσει την πρόσβαση σε αυτό. Θα πρέπει να λάβει υπόψη του τους περιορισμούς στην χρήση του πιστοποιητικού κρυπτογράφησης όπως υποδεικνύονται στον παρόντα Κανονισμό.

Κάθε πληροφορία που θεωρείται κρίσιμη για την έκδοση ενός πιστοποιητικού (π.χ. οι πληροφορίες που υποβάλλονται κατά την Ηλεκτρονική Εγγραφή για πιστοποιητικά, το Έντυπο ΥΔΚ, ή/και τα αρχεία καταγραφής ΑΠ) διατηρούνται για περίοδο 30 ετών σύμφωνα με τον ΚΠ.

Τα πιστοποιητικά απαγορεύεται να χρησιμοποιηθούν για σκοπούς άλλους από εκείνους για τους οποίους εκδόθηκαν.

2.1.5. Υποχρεώσεις Τρίτου Συμμετέχοντα

Οι υποχρεώσεις του Τρίτου Συμμετέχοντα ισχύουν βάσει του παρόντος Κανονισμού μέσω των Όρων Τρίτου Συμμετέχοντα. Οι ισχύοντες Όροι Τρίτου Συμμετέχοντα δημοσιεύονται στη διεύθυνση http://www.syzefxis.gov.gr.

Οι Όροι Τρίτου Συμμετέχοντα "ΟΤΣ" τίθενται σε ισχύ ταυτόχρονα με την υποβολή αιτήματος αναζήτησης ενός Πιστοποιητικού ή επαλήθευσης μίας ψηφιακής υπογραφής, η οποία έχει παραχθεί από ιδιωτικό κλειδί που αντιστοιχεί σε δημόσιο κλειδί το οποίο περιλαμβάνεται σε ένα Πιστοποιητικό, ή με την με οποιοδήποτε άλλο τρόπο χρήση ή στήριξη σε οποιαδήποτε πληροφορία ή υπηρεσία που παρέχεται από το Χώρο Αποθήκευσης ή το δικτυακό χώρο της ΑΠΕΔ σχετικά με ένα Πιστοποιητικό.

Οι ισχύοντες Όροι Τρίτου Συμμετέχοντα περιλαμβάνουν τα κάτωθι:

Ο Τρίτος Συμμετέχων:

1. Αποδέχεται ότι έχει πρόσβαση σε επαρκείς πληροφορίες, οι οποίες του επιτρέπουν να λάβει μία τεκμηριωμένη απόφαση για το κατά πόσον θα βασιστεί σε ένα Πιστοποιητικό ή όχι. Για περισσότερες πληροφορίες ενημερωτικού χαρακτήρα έχει τη δυνατότητα να ανατρέξει στο χώρο αποθήκευσης της ΑΠΕΔ στην ηλεκτρονική διεύθυνση http://www.syzefxis.gov.gr.

2. Αναγνωρίζει και συμφωνεί ότι η εκ μέρους του χρήση του Χώρου Αποθήκευσης της ΑΠΕΔ και η στήριξή του σε οποιοδήποτε Πιστοποιητικό διέπεται από τον Κανονισμό Πιστοποίησης της ΑΠΕΔ, όπως εκάστοτε ισχύει, ο οποίος ενσωματώνεται κατά παραπομπή στους παρόντες Όρους. Ο Κανονισμός Πιστοποίησης δημοσιεύεται στο Διαδίκτυο, στο Χώρο Αποθήκευσης της ΑΠΕΔ στην ηλεκτρονική διεύθυνση http://www.syzefxis.gov.gr. Οι τροποποιήσεις του ΚΠ επίσης, ανακοινώνονται στο Χώρο Αποθήκευσης της ΑΠΕΔ στην ηλεκτρονική διεύθυνση http://www.syzefxis.gov.gr. Οι απαραίτητες από αυτόν ενέργειες για τον έλεγχο της εγκυρότητας ενός Πιστοποιητικού και για την επαλήθευση μιας ηλεκτρονικής υπογραφής περιλαμβάνονται στον ΚΠ.

3. Το Πιστοποιητικό Υπογραφής στο οποίο προτίθεται να βασιστεί ο Τρίτος Συμμετέχων αντιστοιχεί στην ΠΠ 1 του ΚΠ της ΑΠΕΔ και εκδόθηκε σύμφωνα με τις απαιτήσεις που παρατίθενται στο ΠΔ 150/2001 (ΦΕΚ 125/Α) . Ο προσδιοριστής αντικειμένου (Object IDentifier ή 'OID') που αντιστοιχεί στο συγκεκριμένο πιστοποιητικό είναι qcp-public-with-sscd -0.4.0.1456.1.1 σύμφωνα με την πολιτική QCP public + SSCD του κειμένου "ETSI 101 456".

4. Προτού βασιστεί σε μια ψηφιακή υπογραφή η οποία έχει δημιουργηθεί με ιδιωτικό κλειδί που αντιστοιχεί σε δημόσιο κλειδί και το οποίο περιέχεται σε ένα πιστοποιητικό, υποχρεούται να επαληθεύσει την ισχύ, εγκυρότητα, αναστολή ή ανάκληση κάποιου πιστοποιητικού, χρησιμοποιώντας τις τρέχουσες υφιστάμενες πληροφορίες κατάστασης-ανάκλησης πιστοποιητικού.

5. Θα πρέπει να λάβει υπόψη τους περιορισμούς στη χρήση του πιστοποιητικού οι οποίοι υποδεικνύονται για τον Τρίτο Συμμετέχοντα στον ΚΠ.

6. Θα πρέπει να λάβει κάθε άλλη προφύλαξη που υπαγορεύεται από τους παρόντες όρους.

7. Θα πρέπει να λαμβάνει πάντοτε υπόψη την πιθανότητα κλοπής ή άλλης μορφής έκθεσης σε κίνδυνο ενός ιδιωτικού κλειδιού που αντιστοιχεί σε ένα δημόσιο κλειδί, το οποίο περιέχεται σε ένα πιστοποιητικό καθώς και την πιθανότητα να χρησιμοποιηθεί ένα ιδιωτικό κλειδί που έχει κλαπεί ή εκτεθεί σε κίνδυνο για την πλαστογράφηση μιας ψηφιακής υπογραφής σε ένα έγγραφο, ενέργειες οι οποίες δεν είναι πάντα ανιχνεύσιμες. Για πληροφορίες που αφορούν στην προστασία ιδιωτικών κλειδιών, ανατρέχει στην ηλεκτρονική διεύθυνση http://www.syzefxis.gov.gr.

8. Με την υποβολή αιτήματος αναζήτησης ή επαλήθευσης της κατάστασης-ανάκλησης ενός Πιστοποιητικού ή με την με οποιοδήποτε άλλο τρόπο χρήση ή στήριξη σε οποιαδήποτε πληροφορία ή υπηρεσία που παρέχεται από το Χώρο Αποθήκευσης ή το δικτυακό χώρο της ΑΠΕΔ σχετικά με ένα Πιστοποιητικό, ο Τρίτος Συμμετέχων λαμβάνει γνώση και αποδέχεται πλήρως και ανεπιφύλακτα τους ανωτέρω όρους.

9. Εφόσον δεν συμφωνεί με τους ανωτέρω όρους, δεν θα πρέπει να προβεί σε οποιαδήποτε από τις προαναφερόμενες ενέργειες.

2.1.6. Υποχρεώσεις Χώρου Αποθήκευσης

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) διασφαλίζει τη λειτουργία χώρου αποθήκευσης για τις υποκείμενες ΑΠ (ΥπΑΠ). Τόσο η ΑΠΕΔ όσο και οι ΥπΑΠ θα δημοσιεύουν ένα δημόσια προσβάσιμο Κατάλογο Ανακληθέντων Πιστοποιητικών τους (ΚΑΠ-CRL).

Με την ανάκληση ενός Πιστοποιητικού Τελικού Χρήστη, οι ΥπΑΠ δημοσιεύουν αναγγελία της ανάκλησης αυτής στον χώρο αποθήκευσης.

2.2. Ευθύνη

2.2.1. Ευθύνη της Αρχής Πιστοποίησης

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) χρησιμοποιεί τους ΟΧΠ και τους ΟΤΣ που αναφέρονται στον ΚΠ §2.1.4, §2.1.5. Οι όροι που ισχύουν για τους Τρίτους Συμμετέχοντες θα περιλαμβάνονται επίσης στους ΟΧΠ των τελικών χρηστών επιπλέον των ΟΤΣ, διότι οι Τελικοί Χρήστες συχνά ενεργούν ως Τρίτοι Συμμετέ-

χοντες.

Η ΑΠΕΔ διασφαλίζει στους Τελικούς Χρήστες και Τρίτους Συμμετέχοντες τα παρακάτω:

- Το Πιστοποιητικά που χορηγούνται βάσει της ΠΠ1 και της ΠΠ2 του παρόντος περιέχουν όλα τα στοιχεία που προβλέπονται στο ΠΔ 150/2001 (ΦΕΚ 125/ 25-06-2001).
- Οι πληροφορίες που περιλαμβάνονται ή ενσωματώνονται στο Πιστοποιητικό αυτό είναι ακριβείς και αληθείς.
- Στην περίπτωση Πιστοποιητικών που εμφανίζονται στο Χώρο Αποθήκευσης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ), έχουν εκδοθεί προς το φυσικό πρόσωπο που αναγράφεται σε αυτά ως Τελικός Χρήστης και ότι ο Τελικός Χρήστης έχει αποδεχθεί αυτά τα Πιστοποιητικά σύμφωνα με την § 4.3 του ΚΠ.
- Οι Αρχές Εγγραφής (και τα υποκείμενα αυτών Εντεταλμένα Γραφεία) έχουν συμμορφωθεί πλήρως με τον παρόντα ΚΠ κατά την έκδοση ενός Πιστοποιητικού.
- Ο Τελικός Χρήστης του Πιστοποιητικού Υπογραφής ήταν κάτοχος του ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί του Πιστοποιητικού αυτού κατά το χρόνο έκδοσης του τελευταίου.
- Η ΥπΑΠ επιδεικνύει κάθε εύλογη επιμέλεια για να παρέχει ειδοποίηση για την ανάκληση Πιστοποιητικών σύμφωνα με τις § 4.4.9, § 4.4.11 του ΚΠ.

2.2.2. Ευθύνη της Αρχής Εγγραφής και των Εντεταλμένων Γραφείων

Κάθε Αρχή Εγγραφής από κοινού με τα αρμόδια Εντεταλμένα Γραφεία διασφαλίζουν την επαλήθευση της ταυτότητας του τελικού χρήστη και υπέχουν σχετική ευθύνη ενώπιον της ΑΠ.

2.2.3. Υποχρεώσεις του Τελικού Χρήστη

Οι Όροι Χορήγησης Πιστοποιητικού της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) απαιτούν από τους Τελικούς Χρήστες να διασφαλίζουν ότι:

- Κάθε ψηφιακή υπογραφή που δημιουργείται χρησιμοποιώντας το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο Πιστοποιητικό Υπογραφής (ΠΠ 1), αποτελεί την ψηφιακή υπογραφή του Τελικού Χρήστη.
- Κανένα μη-εξουσιοδοτημένο πρόσωπο δεν είχε ποτέ πρόσβαση σε ιδιωτικό κλειδί του Τελικού Χρήστη.
- Όλα τα στοιχεία που παρέχονται από τον Τελικό Χρήστη κατά την Ηλεκτρονική Εγγραφή για πιστοποιητικά στο «Εντυπο ΥΔΚ" είναι αληθή.
- Όλες οι πληροφορίες που παρέχονται από τον Τελικό Χρήστη και περιλαμβάνονται σε ένα Πιστοποιητικό είναι αληθείς.
- Τα Πιστοποιητικά χρησιμοποιούνται αποκλειστικά για εγκεκριμένους και σύννομους σκοπούς, σύμφωνα με τον παρόντα ΚΠ.

2.2.3.1. Έκθεση σε Κίνδυνο του Ιδιωτικού Κλειδιού

Οι προδιαγραφές για την προστασία των ιδιωτικών κλειδιών των τελικών χρηστών, περιλαμβάνονται βάσει της § 6.2 του ΚΠ στους Όρους Χορήγησης Πιστοποιητικού. Οι Τελικοί Χρήστες υποχρεούνται να τηρούν τις προδιαγραφές αυτές.

2.2.4. Υποχρεώσεις Τρίτου Συμμετέχοντα

Οι Τρίτοι Συμμετέχοντες υποχρεούνται να τηρούν τους Όρους Τρίτου Συμμετέχοντα, σύμφωνα με την § 2.1.5. του ΚΠ.

2.3. Ευθύνη Τελικών Χρηστών και Τρίτων Συμμετεχόντων

2.3.1. Ευθύνη Τελικού Χρήστη

Οι Τελικοί Χρήστες υπέχουν ευθύνη ενώπιον των ΥπΑΠ και της ΑΠΕΔ, για τυχόν :

- Ψευδή ή παραποιημένα στοιχεία που υποβλήθηκαν από τον Τελικό Χρήστη στην Ηλεκτρονική Εγγραφή του για πιστοποιητικά.
- Παράλειψη του Τελικού Χρήστη να προστατεύσει το ιδιωτικό του κλειδί, να χρησιμοποιήσει αξιόπιστο σύστημα ή να λάβει τις προφυλάξεις που είναι απαραίτητες ώστε να αποτραπεί έκθεση σε κίνδυνο του ιδιωτικού του κλειδιού, απώλεια, αποκάλυψη, τροποποίηση ή μη-εξουσιοδοτημένη χρήση του.
- Χρήση ονόματος από τον Τελικό Χρήστη (περιλαμβανομένων ενδεικτικά κοινού ονόματος, ονόματος τοποθεσίας διαδικτύου ή διεύθυνσης ηλεκτρονικού ταχυδρομείου) η οποία παραβιάζει τα δικαιώματα περί πνευματικής ιδιοκτησίας οποιουδήποτε τρίτου προσώπου.

2.3.2. Ευθύνη Τρίτου Συμμετέχοντα

Κάθε τρίτος Συμμετέχων υπέχει ευθύνη ενώπιον των ΥπΑΠ και της ΑΠΕΔ, για τυχόν :

- Παράλειψή του να εκτελέσει τις υποχρεώσεις του (ως Τρίτος Συμμετέχων),
- Στήριξή του σε Πιστοποιητικό, η οποία δεν ήταν εύλογη σύμφωνα με τις περιστάσεις,
- Παράλειψή του να ελέγξει την κατάσταση Πιστοποιητικού ώστε να προσδιορίσει εάν το Πιστοποιητικό έχει λήξει ή ανακληθεί.

2.4. Διαχειριστικές Διαδικασίες

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) διασφαλίζει τη συνεχή παροχή των υπηρεσιών της.

2.4.1. Ερμηνεία και Εφαρμογή

2.4.1.1. Εφαρμοστέο Δίκαιο

Ο παρών ΚΠ διέπεται αποκλειστικά από την ελληνική και κοινοτική νομοθεσία.

2.5. Τέλη

2.5.1. Τέλη Έκδοσης ή Ανανέωσης Πιστοποιητικού

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δεν χρεώνει τους τελικούς χρήστες για την έκδοση, το χειρισμό και την ανανέωση Πιστοποιητικών.

2.5.2. Τέλη για την Πρόσβαση σε Πιστοποιητικό

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δεν χρεώνει τέλη για τη διαθεσιμότητα ενός Πιστοποιητικού σε χώρο αποθήκευσης ή για τη με άλλον τρόπο διαθεσιμότητα Πιστοποιητικών προς τους Τρίτους Συμμετέχοντες.

2.5.3. Τέλη για την Πρόσβαση σε Πληροφορίες Ανάκλησης ή Κατάστασης

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δεν χρεώνει τέλη ως προϋπόθεση για τη διαθεσιμότητα ΚΑΠ όπως προβλέπεται από την § 4.4.9 του ΚΠ σε χώρο αποθήκευσης ή για τη με άλλον τρόπο διαθεσιμότητα ΚΑΠ προς Τρίτους Συμμετέχοντες. Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δεν επιτρέπει την πρόσβαση σε πληροφορίες ανάκλησης ή κατάστασης Πιστοποιητικού στο χώρο αποθήκευσής της σε τρίτα πρόσωπα τα οποία παρέχουν προϊόντα ή υπηρεσίες και κάνουν χρήση αυτών των πληροφοριών χωρίς την προηγούμενη ρητή συγκατάθεση της.

2.5.4. Τέλη για Άλλες Υπηρεσίες όπως οι Πληροφορίες Πολιτικής

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δεν χρεώνει τέλη για την πρόσβαση στον παρόντα ΚΠ. Οποι-

αδήποτε χρήση γίνεται για σκοπούς διαφορετικούς από την απλή ανάγνωση αυτών των εγγράφων, όπως είναι η αναπαραγωγή, αναδιανομή, τροποποίηση ή δημιουργία αντιγράφων απαιτεί προηγούμενη άδεια από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) Α.Ε. η οποία κατέχει τα δικαιώματα πνευματικής ιδιοκτησίας.

2.6. Δημοσίευση και Χώρος Αποθήκευσης

2.6.1. Δημοσίευση Πληροφοριών

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) διασφαλίζει τη λειτουργία ηλεκτρονικού χώρου αποθήκευσης για:

- Την Πρωτεύουσα Αρχή Πιστοποίησης (ΑΠΕΔ).
- Τις Αρχές Πιστοποίησης οι οποίες εκδίδουν Πιστοποιητικά τελικών χρηστών (ΥπΑΠ).

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δημοσιεύει πληροφορίες για τις ΑΠ στο χώρο αποθήκευσης που βρίσκεται στον δικτυακό της κόμβο, στη διεύθυνση http://www.syzefxis.gov.gr όπως περιγράφεται παρακάτω.

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δημοσιεύει τον παρόντα ΚΠ, τους ΟΧΠ, τους ΟΤΣ και πληροφορίες ανάκλησης σχετικά με τα πιστοποιητικά που εκδίδει στο χώρο αποθήκευσης που βρίσκεται στο δικτυακό της κόμβο.

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δημοσιεύει Πιστοποιητικά σύμφωνα με τον ακόλουθο Πίνακα 2α.

Πίνακας 2α- Απαιτήσεις Δημοσίευσης Πιστοποιητικών	
Μορφή Πιστοποιητικού	Απαιτήσεις Δημοσίευσης
Πιστοποιητικά Αρχής Πιστοποίησης Ελληνικού Δημοσίου	Διαθέσιμα στους Τρίτους Συμμετέχοντες, διαδικτυακά μέσω του χώρου αποθήκευσής της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) στο http://www.syzefxis.gov.gr καθώς και ως μέρος της Αλυσίδας Πιστοποιητικού η οποία ενσωματώνεται στο Πιστοποιητικό Τελικού Χρήστη μέσω των λειτουργιών αναζήτησης που περιγράφονται παρακάτω.

Οι ΥπΑΠ δημοσιεύουν Πιστοποιητικά σύμφωνα με τον ακόλουθο Πίνακα 2β

Πίνακας 2β - Απαιτήσεις Δημοσίευσης Πιστοποιητικών	
Μορφή Πιστοποιητικού	Απαιτήσεις Δημοσίευσης
Πιστοποιητικά Τελικού Χρήστη	Διαθέσιμα προς τους Τρίτους Συμμετέχοντες μέσω λειτουργιών αναζήτησης στο χώρο αποθήκευσης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) στη διεύθυνση http://www.syzefxis.gov.gr
	Επίσης διαθέσιμα μέσω αναζήτησης στο server του καταλόγου LDAP της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)

2.6.2. Συχνότητα Δημοσίευσης

Ενημερωμένες εκδόσεις του παρόντα ΚΠ δημοσιεύονται σύμφωνα με την § 8 του ΚΠ. Ενημερωμένες εκδόσεις των ΟΧΠ και των ΟΤΣ δημοσιεύονται στη διεύθυνση http://www.syzefxis.gov.gr. Τα Πιστοποιητικά δημοσιεύονται κατά την έκδοση. Πληροφορίες αναφορικά με την κατάσταση Πιστοποιητικών δημοσιεύονται σύμφωνα με τις §4.4.9 και §4.4.11 του ΚΠ.

2.6.3. Έλεγχοι Πρόσβασης

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) διασφαλίζει την εφαρμογή και υλοποίηση λογικών και φυσικών μέτρων ασφαλείας προκειμένου να αποτραπεί η προσθήκη, διαγραφή ή τροποποίηση των καταχωρήσεων στο χώρο αποθήκευσης από μη εξουσιοδοτημένα πρόσωπα.

Ουσιαστικός όρος για την καταχώρηση στο χώρο αποθήκευσης οποιαδήποτε αλλαγής π.χ. αποδοχή του αιτήματος ανανέωσης ενός Πιστοποιητικού Τελικού Χρήστη είναι η επιβεβαίωση των πληροφοριών ταυτοποίησης φυσικού προσώπου και πιστοποιητικού του τελικού χρήστη. Σε αντίθετη περίπτωση επαναλαμβάνεται η διαδικασία που προβλέπεται στην §3.1.7 του ΚΠ.

2.6.4. Χώροι Αποθήκευσης

Βλ. ΚΠ § 2.1.6.

2.7. Έλεγχος Συμμόρφωσης

Διενεργείται ετήσιος εσωτερικός έλεγχος των υπηρεσιών πιστοποίησης και διαχείρισης κλειδιών που παρέχονται από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) σύμφωνα με τις προδιαγραφές της ΕΕΤΤ. Επιπρόσθετα προς τους ελέγχους συμμόρφωσης, η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) έχει δικαίωμα να διενεργεί και άλλες επιθεωρήσεις ή έρευνες ώστε να εξασφαλίσει την αξιοπιστία των υπηρεσιών που παρέχει. Οι επιθεωρήσεις αυτές περιλαμβάνουν ενδεικτικά διενέργεια «Εκτάκτων Ελέγχων» ή «Επιπρόσθετες Επιθεωρήσεις Διαχείρισης Κινδύνου», ιδίως εφόσον προκύψουν ελλείψεις ή ελαττώματα κατά τον Έλεγχο Συμμόρφωσης.

Οι Φορείς και τα νομικά πρόσωπα που υπόκεινται σε έλεγχο, επιθεώρηση ή έρευνα θα πρέπει να συνεργάζονται με την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και το προσωπικό που διενεργεί τον έλεγχο, την επιθεώρηση ή την έρευνα.

2.7.1. Συχνότητα Ελέγχου Συμμόρφωσης Φορέα

Οι έλεγχοι συμμόρφωσης διενεργούνται σε ετήσια βάση.

2.7.1.1. Θέματα που Καλύπτει ο Έλεγχος

Αντικείμενο του ετησίου ελέγχου αποτελούν τα μέτρα ασφάλειας που λαμβάνονται, οι υπηρεσίες διαχείρισης κλειδιών και τα μέτρα ελέγχου της υποδομής δημοσίου κλειδιού.

2.7.1.2. Λήψη Μέτρων ως Αποτέλεσμα Ανεπάρκειας

Εάν κατά τη διάρκεια του Ελέγχου Συμμόρφωσης αποκαλυφθούν σημαντικές ελλείψεις ή ανεπάρκειες επιβάλλεται να ληφθούν τα απαιτούμενα μέτρα. Ο

προσδιορισμός των μέτρων αυτών θα γίνει από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) κατόπιν της εισήγησης του ελεγκτή. Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) είναι σε κάθε περίπτωση αρμόδια για την ανάπτυξη και εφαρμογή αυτού του επανορθωτικού σχεδίου δράσης εντός εύλογου χρονικού διαστήματος.

2.8. Εμπιστευτικότητα και Προστασία Εμπιστευτικών Πληροφοριών

Η Υποδομή Δημοσίου Κλειδιού βάσει των διατάξεων του παρόντος υπόκειται στην νομοθεσία περί προστασίας των προσωπικών δεδομένων.

2.8.1. Κατηγορίες Πληροφοριών που Θεωρούνται Εμπιστευτικές και Προσωπικές

Εν προκειμένω εφαρμόζονται οι διατάξεις για την πρόσβαση σε διοικητικά έγγραφα, τη προστασία των προσωπικών δεδομένων, του απορρήτου των επικοινωνιών και κάθε άλλη σχετική διάταξη.

2.8.2. Εμπιστευτικότητα

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) αποκαλύπτει Εμπιστευτικές Πληροφορίες σύμφωνα με το Νόμο και κατόπιν σχετικής εισαγγελικής παραγγελίας. Τα ιδιωτικά κλειδιά των πιστοποιητικών υπογραφής τελικών χρηστών που ακολουθούν την ΠΠ 1, δεν αποκαλύπτονται ποτέ σε τρίτο, συμπεριλαμβανομένης και της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ).

2.9. Δικαιώματα Πνευματικής Ιδιοκτησίας

2.9.1. Δικαιώματα Πνευματικής Ιδιοκτησίας στα Πιστοποιητικά και Πληροφορίες Ανάκλησης

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) διατηρεί όλα τα δικαιώματα πνευματικής ιδιοκτησίας για τα πιστοποιητικά και τις πληροφορίες ανάκλησης που εκδίδει. Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) εκχωρεί μη-αποκλειστική, χωρίς χρέωση άδεια αναπαραγωγής και διανομής Πιστοποιητικών εφόσον αυτά αναπαράγονται πλήρως και εφόσον η χρήση τους υπόκειται στους ΟΤΣ. Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) χορηγεί πληροφορίες ανάκλησης σε κάθε Τρίτο Συμμετέχοντα σύμφωνα με τους ισχύοντες ΟΤΣ.

2.9.2. Δικαιώματα Ιδιοκτησίας επί των Κλειδιών και του Υλικού Κλειδιών

Τα δημόσια κλειδιά των τελικών χρηστών αποτελούν πνευματική ιδιοκτησία της ΑΠΕΔ.

2.10. Διαδικασίες για την προστασία Τελικών Χρηστών ή Τρίτων Συμμετεχόντων

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) διασφαλίζει τον Τελικό Χρήστη ή Τρίτο Συμμετέχοντα από αστοχίες της Υποδομής Δημοσίου Κλειδιού βάσει των διατάξεων του παρόντος.

3. Αναγνώριση και Ταυτοποίηση

3.1. Αρχική Εγγραφή

3.1.1. Τύποι Ονομάτων

Τα Πιστοποιητικά που εκδίδει η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) για την πιστοποίηση των ΥπΑΠ, περιλαμβάνουν Διακριτικά Ονόματα X.501 στα πεδία Εκδότη και Υποκειμένου. Τα Διακριτικά Ονόματα των ΥπΑΠ της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) αποτελούνται από τα στοιχεία που προσδιορίζονται παρακάτω στον Πίνακα 3.

Χαρακτηριστικά	Τιμή
Country © - Χώρα=	"GR"
Organization (O)- Οργανισμός=	"Hellenic Public Administration Root Certification Authority HPARCA", Αρχή Πιστοποίησης Ελληνικού Δημοσίου
Organizational Unit (OU) - Οργανική Μονάδα=	Τα Πιστοποιητικά ΥπΑΠ της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δύναται να περιέχουν ένα ή περισσότερα OU. Το περιεχόμενο αυτών μπορεί να σχετίζεται με την χρήση των Πιστοποιητικών αυτών (π.χ. "For Public Services Use Only" εάν η χρήση επιτρέπεται μόνο για το Δημόσιο τομέα).
Common Name (CN)- Κοινό Όνομα=	Το χαρακτηριστικό αυτό περιλαμβάνει το Όνομα ΥπΑΠ (CA name)

Πίνακας 3 - Χαρακτηριστικά Διακριτικού Ονόματος σε Πιστοποιητικά ΥπΑΠ

Τα Πιστοποιητικά Τελικού Χρήστη περιλαμβάνουν διακριτικό όνομα X.501 στο πεδίο ονόματος Υποκειμένου και αποτελούνται από τα στοιχεία που προσδιορίζονται στον Πίνακα 4 παρακάτω.

Χαρακτηριστικά	Τιμή
Country © - Χώρα=	"GR "
Organization (O)- Οργανισμός=	Το Όνομα της ΥπΑΠ που έχει αναλάβει την έκδοση πιστοποιητικών προς τελικούς χρήστες.
Organizational Unit (OU) - Οργανική Μονάδα=	Τα Πιστοποιητικά Τελικού Χρήστη της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δύναται να περιέχουν ένα ή περισσότερα OU. Το περιεχόμενο αυτών μπορεί να σχετίζεται με την χρήση των Πιστοποιητικών αυτών.
Common Name (CN) - Κοινό Όνομα=	Το χαρακτηριστικό αυτό περιλαμβάνει το Ονοματεπώνυμο του Τελικού Χρήστη.
E-Mail Address (E) - Ηλεκτρονική Διεύθυνση=	Διεύθυνση ηλεκτρονικού ταχυδρομείου (e-mail) του Τελικού Χρήστη

Πίνακας 4 - Χαρακτηριστικά Διακριτικού Ονόματος σε Πιστοποιητικά Τελικού Χρήστη

3.1.2. Ανάγκη Κατανόησης των Ονομάτων

Τα ονόματα που περιλαμβάνονται στα Πιστοποιητικά Τελικού Χρήστη βρίσκονται σε μορφή απλή και κατανοητή ώστε να επιτρέπουν τον προσδιορισμό της ταυτότητας του φυσικού προσώπου που αποτελεί το Υποκείμενο του Πιστοποιητικού. Επίσης διασφαλίζεται

η τήρηση των διατάξεων της κείμενης νομοθεσίας για την προστασία των προσωπικών δεδομένων κατά τη διαδικασία εγγραφής.

3.1.3. Κανόνες για την Ερμηνεία των Διαφόρων Τύπων Ονομάτων

Δεν προβλέπεται.

3.1.4. Μοναδικότητα των Ονομάτων

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) διασφαλίζει ότι τα Διακριτικά Ονόματα Υποκειμένου είναι μοναδικά μέσω αυτοματοποιημένων διαδικασιών κατά τη διαδικασία εγγραφής των Τελικών Χρηστών.

3.1.5. Διαδικασία Επίλυσης Διαφορών για τη Χρήση Ονόματος

Δεν ισχύει

3.1.6. Μέθοδος Απόδειξης της Κατοχής Ιδιωτικού Κλειδιού

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) επαληθεύει ότι ο ενδιαφερόμενος Τελικός Χρήστης κατέχει το ιδιωτικό κλειδί υπογραφής μέσω της χρήσης ψηφιακά υπογραφόμενου αιτήματος πιστοποιητικού σύμφωνα με το PKCS #10 (Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού), άλλη ισοδύναμη κρυπτογραφικά μορφή ή άλλη μέθοδο εγκεκριμένη από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ).

3.1.7. Ταυτοποίηση Στοιχείων Φυσικού Προσώπου

Για όλα τα Πιστοποιητικά φυσικών προσώπων, τα αρμόδια Εντεταλμένα Γραφεία και οι Αρχές Εγγραφής των Υποκείμενων Αρχών Πιστοποίησης, επιβεβαιώνουν ότι:

- Ο Τελικός Χρήστης είναι το πρόσωπο που προσδιορίζεται στην Ηλεκτρονική Εγγραφή για Πιστοποιητικά.
- Ο Τελικός Χρήστης διαθέτει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο Πιστοποιητικό σύμφωνα με την§ 3.1.6. του ΚΠ.
- Οι πληροφορίες που περιλαμβάνονται στο Πιστοποιητικό είναι ακριβείς.
- Η πιστοποίηση της ταυτότητας του τελικού χρήστη βασίζεται στην άμεση προσωπική (φυσική) παρουσία του ενδιαφερόμενου Τελικού Χρήστη στο αρμόδιο Εντεταλμένο Γραφείο όπου ελέγχεται η ταυτότητα του από το δελτίο αστυνομικής του ταυτότητας ή άλλο επίσημο έγγραφο παραστατικό της ταυτότητας του προσώπου που φέρει επικυρωμένη φωτογραφία.
- Τα απαιτούμενα δικαιολογητικά που υποβάλλονται από τον Τελικό Χρήστη είναι:

ο δελτίο αστυνομικής ταυτότητας ή άλλο επίσημο έγγραφο παραστατικό της ταυτότητας του προσώπου που φέρει επικυρωμένη φωτογραφία,

ο επικυρωμένη φωτοτυπία του παραπάνω εγγράφου (για το αρχείο του Εντεταλμένου Γραφείου),

ο η έξυπνη κάρτα που του έχει επιδοθεί από τον Προϊστάμενό του έτσι ώστε να παραλάβει τον σφραγισμένο φάκελο που αντιστοιχεί σε αυτή την κάρτα όπου περιέχονται οι μυστικοί αριθμοί πρόσβασης σε αυτή (PIN-PUK/Personal Identification Number - Personal Unblocking Key).

Η προσωπική φυσική παρουσία του ενδιαφερόμενου τελικού χρήστη σε αρμόδιο Εντεταλμένο Γραφείο λαμβάνει χώρα πριν την αποδοχή των ΟΧΠ και την υποβολή της Ηλεκτρονικής Εγγραφής για Πιστοποιητικά.

3.2. Τακτική Επαναδημιουργία Κλειδιών και Ανανέωση

Ο Τελικός Χρήστης πριν από τη λήξη των Πιστοποιητικών του είναι απαραίτητο να αποκτήσει ένα νέο ζεύγος πιστοποιητικών ώστε να διασφαλίσει τη συνέχεια της χρήσης τους. Γι αυτό η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) απαιτεί από τον Τελικό Χρήστη να δημιουργήσει ένα νέο ζεύγος κλειδιών υπογραφής το οποίο θα αντικαταστήσει το ζεύγος κλειδιών υπογραφής που λήγει (τεχνικά ορίζεται ως «επαναδημιουργία κλειδιών»). Ο Πίνακας 5 παρακάτω περιγράφει τις απαιτήσεις της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ).

Μορφή Πιστοποιητικού	Απαιτήσεις Τακτικής Επαναδημιουργίας Κλειδιών και Ανανέωσης
Πιστοποιητικά Τελικού Χρήστη	Ουσιαστικός όρος για την αποδοχή της ανανέωσης ενός Πιστοποιητικού Τελικού Χρήστη είναι ο έλεγχος των πληροφοριών που διενεργείται από την ΥπΑΠ για να επιβεβαιωθεί ότι η ταυτότητα του Τελικού Χρήστη είναι ακόμα έγκυρη. Αυτή η διαδικασία γίνεται με σκοπό να επιβεβαιωθεί ότι το πρόσωπο που επιδιώκει να ανανεώσει ένα πιστοποιητικό Τελικού Χρήστη είναι στην πραγματικότητα ο Τελικός Χρήστης του πιστοποιητικού, όπως αναφέρεται στην § 3.1.7 του ΚΠ.
Πιστοποιητικά ΑΠΕΔ	Παρέχεται η δυνατότητα τόσο της επαναδημιουργίας κλειδιών σύμφωνα με την § 4.7 του ΚΠ όσο και της ανανέωσης πιστοποιητικών χωρίς την υποχρέωση επαναδημιουργίας του ζεύγους κλειδιών, εφόσον ο αθροιστικός πιστοποιημένος χρόνος ζωής του ζεύγους κλειδιών της ΥπΑΠ δεν υπερβαίνει το εκάστοτε ανώτερο όριο διάρκειας ισχύος ζεύγους κλειδιών ΥπΑΠ όπως καθορίζεται στην § 6.3.2 του ΚΠ. Για παράδειγμα, εάν ένα πιστοποιητικό με το οποίο πιστοποιείται μία ΥπΑΠ έχει εκδοθεί για χρόνο ζωής 3 ετών, δύναται να παραταθεί η περίοδος ισχύος του ζεύγους κλειδιών της ΥπΑΠ για 2 επιπλέον έτη, καλύπτοντας την ανώτατη επιτρεπόμενη περίοδο ισχύος των 5 ετών.

Πίνακας 5 - Απαιτήσεις Τακτικής Επαναδημιουργίας Κλειδιών και Ανανέωσης

3.2.1. Τακτική Επαναδημιουργία Κλειδιών και Ανανέωση για Πιστοποιητικά Τελικού Χρήστη

Για τα Πιστοποιητικά Τελικού Χρήστη, τα οποία δεν έχουν ανακληθεί, είναι δυνατή η αντικατάστασή τους (δηλαδή η επαναδημιουργία κλειδιών τους) σύμφωνα με τα ακόλουθα:

1. Το αρμόδιο Εντεταλμένο Γραφείο θα πρέπει να επαναβεβαιώσει την ταυτότητα του Τελικού Χρήστη σύμφωνα με τις απαιτήσεις που ορίζονται στην § 3.1.7 του ΚΠ.

2. Ο χρήστης ενημερώνεται μέσω μηνύματος ηλεκτρονικού ταχυδρομείου (email) από τον Υπεύθυνο της Αρχής Εγγραφής ότι πρέπει να γίνει ανανέωση των πιστοποιητικών του (υπογραφής-κρυπτογράφησης) το αργότερο δεκαπέντε (15) ημέρες πριν από την λήξη τους.

3. Ο χρήστης υποβάλει ηλεκτρονικό αίτημα για Ανανέωση των πιστοποιητικών του το οποίο θα πρέπει να αποδεχθεί ο Υπεύθυνος της Αρχής Εγγραφής αφού προηγουμένως ελέγξει την ορθότητα των στοιχείων της Ηλεκτρονικής Αίτησης.

3.2.2. Τακτική Επαναδημιουργία Κλειδιών και Ανανέωση για Πιστοποιητικά ΥπΑΠ

Οι ΥπΑΠ δύναται να ακολουθούν διαδικασίες επαναδημιουργίας κλειδιών περιοδικά σύμφωνα με την § 4.7 του ΚΠ.

3.3. Επαναδημιουργία Κλειδιών Μετά την Ανάκληση

Η Επαναδημιουργία Κλειδιών μετά την ανάκληση δεν είναι δυνατή εφόσον:

- Η ανάκληση συνέβη επειδή τα Πιστοποιητικά εκδόθηκαν προς πρόσωπο διαφορετικό από αυτό το οποίο κατονομάζεται ως το Υποκείμενο του Πιστοποιητικού.
- Τα Πιστοποιητικά εκδόθηκαν χωρίς τη συγκατάθεση του προσώπου το οποίο κατονομάζεται ως Υποκείμενο τους.
- Το πρόσωπο το οποίο εγκρίνει την Ηλεκτρονική Εγγραφή του Τελικού Χρήστη για Πιστοποιητικά ανακαλύπτει ή έχει λόγο να πιστεύει ότι ορισμένα ουσιώδη στοιχεία στην Ηλεκτρονική Εγγραφή για Πιστοποιητικά είναι ψευδή.

Υπό τους όρους της προηγούμενης παραγράφου, τα Πιστοποιητικά Τελικού Χρήστη, τα οποία έχουν ανακληθεί, είναι δυνατόν να αντικατασταθούν (να επαναδημιουργηθούν τα ζεύγη κλειδιών), σύμφωνα με τις § 3.3.1, § 3.1.7 του ΚΠ.

3.3.1. Αίτημα Ανάκλησης

Για την ανάκληση πιστοποιητικών τελικών χρηστών ακολουθείται η παρακάτω διαδικασία:

1. Ο Τελικός Χρήστης πρέπει να ενημερώσει το αρμόδιο Εντεταλμένο Γραφείο ("Εντυπο ΥΔΚ"), το οποίο θα επαληθεύσει το αίτημα του, για τους λόγους ανάκλησης του Πιστοποιητικού του.

2. Ο Υπεύθυνος του Εντεταλμένου Γραφείου υποχρεούται να ενημερώσει άπαξ ημερησίως μέσω υπογεγραμμένου μηνύματος ηλεκτρονικού ταχυδρομείου τον Υπεύθυνο της υπερκείμενης Αρχής Εγγραφής σχετικά με τις αιτήσεις ανάκλησης που έχουν υποβληθεί.

3. Ο Υπεύθυνος της Αρχής Εγγραφής μέσω ασφαλούς σύνδεσης έχει δυνατότητα να ανακαλέσει τα απαιτούμενα πιστοποιητικά ενημερώνοντας αυτόματα τον Κατάλογο Ανακληθέντων Πιστοποιητικών (CRL) της ΥπΑΠ που τα υπέγραψε.

4. Οι Υπεύθυνοι των Αρχών Εγγραφής έχουν δικαίωμα να ζητήσουν την ανάκληση Πιστοποιητικών Τελικού Χρήστη.

Οι λόγοι ανάκλησης πιστοποιητικών παρατίθενται στην § 4.4.1.1 του ΚΠ.

3.3.2. Αίτημα Ανάκτησης Πιστοποιητικού Κρυπτογράφησης

Η διαδικασία για την ανάκτηση κάποιου πιστοποιητικού κρυπτογράφησης είναι η ακόλουθη:

1. Ο Τελικός Χρήστης θα πρέπει να μεταβεί αυτοπροσώπως στο Εντεταλμένο Γραφείο από το οποίο έχει ταυτοποιηθεί και να συμπληρώσει την αίτηση ανάκτησης πιστοποιητικού κρυπτογράφησης ("Εντυπο ΥΔΚ") στην οποία δηλώνει τον λόγο για τον οποίο αιτείται την ανάκτηση.

2. Ο Υπεύθυνος του Εντεταλμένου Γραφείου ταυτοποιεί τον αιτούντα και ενημερώνει τον Υπεύθυνο της αρμόδιας Αρχής Εγγραφής ο οποίος μπορεί να προβεί στην ανάκτηση του πιστοποιητικού.

4. Λειτουργικές Απαιτήσεις

4.1. Διαδικασίες για τη χορήγηση Πιστοποιητικού

4.1.1. Διαδικασίες για τη χορήγηση Πιστοποιητικού Τελικού Χρήστη

Για τα Πιστοποιητικά της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ), όλοι οι Τελικοί Χρήστες υποβάλλονται σε διαδικασία εγγραφής η οποία συνίσταται σε:

- Παραλαβή της έξυπνης κάρτας από τον προϊστάμενο του Τελικού Χρήστη.
- Παραλαβή από το Εντεταλμένο Γραφείο του σφαγισμένου φακέλου όπου περιέχονται οι κωδικοί πρόσβασης (PIN-PUK / Personal Identification Number - Personal Unblocking Key) στην έξυπνη κάρτα.
- Συμπλήρωση και υπογραφή του «Εντύπου ΥΔΚ», παροχή των απαραίτητων πληροφοριών και υποβολή στοιχείων ταυτοποίησης σύμφωνα με την§ 3.1.7 ΚΠ. Οι πληροφορίες αυτές θα περιλαμβάνουν στοιχεία διεύθυνσης τα οποία θα επιτρέπουν στην ΥπΑΠ να επικοινωνήσει με τον Τελικό Χρήστη.
- Αποδοχή των Όρων Χορήγησης Πιστοποιητικού (ΟΧΠ) που περιλαμβάνονται στο "Εντυπο ΥΔΚ" και βρίσκονται σε συμφωνία με τα προβλεπόμενα που περιγράφονται στην § 2.1 του ΚΠ.
- Υποβολή Ηλεκτρονικού αιτήματος για πιστοποιητικά (υπογραφής-κρυπτογράφησης).
- Παραγωγή ή υποβολή αιτήματος για παραγωγή ζεύγους κλειδιών υπογραφής -κρυπτογράφησης σύμφωνα με την § 6.1 του ΚΠ.
- Αποστολή του δημόσιου κλειδιού από τον Τελικό Χρήστη, σε ΥπΑΠ της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ), σύμφωνα με την § 6.1.3 του ΚΠ.
- Ο Τελικός Χρήστης αποδεικνύει στην ΥπΑΠ σύμφωνα με την § 3.1.6 του ΚΠ ότι έχει στην κατοχή του το ιδιωτικό κλειδί υπογραφής που αντιστοιχεί στο δημόσιο κλειδί που απέστειλε στην ΥπΑΠ.

Τα αρχεία που διατηρούνται σύμφωνα με την § 4.6.1 του ΚΠ περιλαμβάνουν τις πληροφορίες που χρησιμοποιούνται για να ταυτοποιήσουν τον Τελικό Χρήστη (συμπεριλαμβανομένου οιουδήποτε αριθμού αναφοράς που χρησιμοποιείται για την ταυτοποίηση) καθώς και ένα αρχείο των ΟΧΠ είτε σε χαρτί είτε σε ηλεκτρονική μορφή.

Τα «Εντυπα ΥΔΚ» υποβάλλονται στα αρμόδια Εντεταλμένα Γραφεία, για επεξεργασία (αποδοχή ή απόρριψη). Στη συνέχεια οι διαδικασίες που λαμβάνουν χώρα είναι οι ακόλουθες:

- οι Φορείς που θα διενεργήσουν τη διαδικασία ταυτοποίησης (Εντεταλμένα Γραφεία) έχουν ενημερωθεί από την ΥπΑΠ ή την ΑΕ για τους τελικούς χρήστες που θα εξυπηρετήσουν και έχουν παραλάβει τον απαιτούμενο αριθμό κωδικών PIN-PUK με τους οποίους επιτυγχάνεται πρόσβαση στις έξυπνες κάρτες των εν λόγω τελικών χρηστών.
- Οι Προϊστάμενοι των Τελικών Χρηστών έχουν παραδώσει στους δικαιούχους τις αντίστοιχες έξυπνες κάρτες.

Στην περίπτωση μιας αίτησης για ανανέωση ή επανέκδοση:

- οποιεσδήποτε αλλαγές στους ΟΧΠ μετά από την προηγούμενη εγγραφή ή επανεγγραφή είναι σύμφωνες με την §2.1 του ΚΠ και
- τα αρχεία που διατηρούνται σύμφωνα με την § 4.6.1 του ΚΠ επίσης περιλαμβάνουν τη συγκατάθεση του Τελικού Χρήστη σε οποιεσδήποτε τέτοιες αλλαγές.

4.2. Έκδοση Πιστοποιητικού

4.2.1. Έκδοση Πιστοποιητικού Τελικού Χρήστη

Με την υποβολή του «Εντύπου ΥΔΚ» από τον Τελικό Χρήστη, εξουσιοδοτημένος υπάλληλος της Αρχής Εγγραφής ή του Εντεταλμένου Γραφείου, επιβεβαιώνει τα στοιχεία ταυτοποίησης σύμφωνα με την § 3.1.7 του ΚΠ. Με την επιτυχή τέλεση όλων των απαιτούμενων διαδικασιών ταυτοποίησης, ο Υπεύθυνος της ΑΕ, θα εγκρίνει την Ηλεκτρονική Εγγραφή για πιστοποιητικά. Εφόσον η ταυτοποίηση δεν είναι επιτυχής, αντίστοιχα θα την απορρίψει.

Τα πιστοποιητικά Τελικού Χρήστη δημιουργούνται και εκδίδονται μετά την έγκριση της Ηλεκτρονικής Εγγραφής που υποβάλλεται από τον Τελικό Χρήστη. Η ΥπΑΠ δημιουργεί και εκδίδει πιστοποιητικά προς τον ενδιαφερόμενο Τελικό Χρήστη βάσει των στοιχείων του «Εντύπου ΥΔΚ» και εφόσον έχει εγκρίνει την αντίστοιχη Ηλεκτρονική Εγγραφή για πιστοποιητικά.

Οι διαδικασίες της παραγράφου αυτής ισχύουν επίσης και για την έκδοση πιστοποιητικών μετά από υποβολή αιτήματος αντικατάστασης (δηλαδή ανανέωσης ή επαναδημιουργίας κλειδιών) πιστοποιητικού σύμφωνα με την§ 3.2 ΚΠ.

4.2.2. Έκδοση Πιστοποιητικού ΥπΑΠ

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ) πιστοποιεί Υποκείμενες Αρχές Πιστοποίησης και υπογράφει τα αντίστοιχα πιστοποιητικά Υποκείμενης ΑΠ σύμφωνα με τα προβλεπόμενα στις διατάξεις του άρθρου 20 του Ν.3448/2006 και την §1.2.2 του ΚΠ.

4.3. Αποδοχή Πιστοποιητικού

Η ΥπΑΠ γνωστοποιεί στους Τελικούς Χρήστες ότι τα Πιστοποιητικά τους είναι διαθέσιμα και τους ενημερώνει για τον τρόπο με τον οποίο θα τα λάβουν.

Με την έκδοση, τα Πιστοποιητικά καθίστανται διαθέσιμα στους Τελικούς Χρήστες μέσω μηνύματος το οποίο αποστέλλεται στον Τελικό Χρήστη από την ΥπΑΠ, στο οποίο περιλαμβάνεται ένας προσωπικός κωδικός PIN τον οποίο ο τελικός χρήστης θα εισαγάγει στην ιστοσελίδα εγγραφής προκειμένου να παραλάβει τα πιστοποιητικά του. Για παράδειγμα, η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) μπορεί να αποστείλει στον Τελικό Χρήστη έναν Προσωπικό Κωδικό PIN, τον οποίο ο Τελικός Χρήστης θα εισαγάγει στην ιστοσελίδα εγγραφής προκειμένου να παραλάβει τα Πιστοποιητικά του. Η εγκατάσταση των πιστοποιητικών συνιστά την αποδοχή τους από τον Τελικό Χρήστη.

4.4. Αναστολή και Ανάκληση Πιστοποιητικού

4.4.1. Συνθήκες Ανάκλησης

4.4.1.1. Συνθήκες για Ανάκληση Πιστοποιητικών Τελικού Χρήστη

Ένα Πιστοποιητικό Τελικού Χρήστη ανακαλείται εφόσον:

1. Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) ή η ΥπΑΠ ή ένας Τελικός Χρήστης έχουν σοβαρές υπόνοιες ότι έχει υπάρξει Έκθεση σε Κίνδυνο του ιδιωτικού κλειδιού ενός Τελικού Χρήστη.
2. Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) ή η ΥπΑΠ έχει σοβαρές υπόνοιες ότι ο Τελικός Χρήστης έχει παραβεί ουσιωδώς μια σημαντική υποχρέωση ή εγγύηση σύμφωνα με τους ισχύοντες ΟΧΠ.
3. Υπάρχει απώλεια της έξυπνης κάρτας ή των μυστικών αριθμών PIN-PUK από τον Τελικό Χρήστη.
4. Αδυναμία χρήσης ενός ή και των δύο πιστοποιητικών (υπογραφής ή κρυπτογράφησης) του τελικού χρήστη για τεχνικούς λόγους.
5. Για υπηρεσιακούς λόγους (π.χ. παραίτηση ή αποχώρηση του τελικού χρήστη).
6. Οι ΟΧΠ έχουν τροποποιηθεί και δεν έχουν γίνει αποδεκτοί από τον Τελικό Χρήστη.
7. Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) ή η ΥπΑΠ έχει λόγο να πιστεύει ότι το Πιστοποιητικό έχει εκδοθεί με τρόπο που δεν είναι ουσιαστικά σύμφωνος με τις διαδικασίες που απαιτούνται από τον ισχύοντα ΚΠ, ότι το Πιστοποιητικό εκδόθηκε προς πρόσωπο διαφορετικό από αυτό που κατονομάζεται ως το Υποκείμενο του Πιστοποιητικού ή χωρίς την έγκριση του προσώπου που κατονομάζεται ως το Υποκείμενο του Πιστοποιητικού αυτού.
8. Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) ή η ΥπΑΠ έχει λόγο να πιστεύει ότι κάποιο ουσιαστικό στοιχείο στο «Έντυπο ΥΔΚ» ή την Ηλεκτρονική Αίτηση για πιστοποιητικά είναι ψευδές.
9. Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) ή η ΥπΑΠ αποφαίνεται ότι δεν ικανοποιείται ή υπάρχει απόκλιση από μια βασική προϋπόθεση για την Έκδοση Πιστοποιητικού.
10. Οι πληροφορίες που περιλαμβάνονται στο Πιστοποιητικό είναι ανακριβείς ή έχουν μεταβληθεί.
11. Ο Τελικός Χρήστης έχει ζητήσει ανάκληση του Πιστοποιητικού σύμφωνα με την § 3.3.1. του ΚΠ.

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δύναται να ανακαλέσει ένα Πιστοποιητικό Υπεύθυνου ΑΕ εφόσον η απόφαση βάσει της οποίας του έχουν εκχωρηθεί αυτές οι αρμοδιότητες έχει τροποποιηθεί.

Οι ΟΧΠ της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) απαιτούν από τους Τελικούς Χρήστες να ενημερώσουν άμεσα την ΥπΑΠ εάν γνωρίζουν ή έχουν υπόνοιες για την έκθεση σε κίνδυνο του ιδιωτικού τους κλειδιού σύμφωνα με τις διαδικασίες της § 4.4.3.1 του ΚΠ.

4.4.1.2. Συνθήκες Ανάκλησης Πιστοποιητικών που εκδίδει η ΑΠΕΔ

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) ανακαλεί πιστοποιητικά που εκδίδει για τις ΥπΑΠ, εφόσον:

ο Ανακαλύψει ή έχει λόγο να πιστεύει ότι έχει υπάρξει έκθεση σε κίνδυνο του ιδιωτικού κλειδιού ΥπΑΠ.

ο Ανακαλύψει ή έχει λόγο να πιστεύει ότι το Πιστοποιητικό ΥπΑΠ έχει εκδοθεί με τρόπο που δεν είναι ουσιαστικά σύμφωνος με τις διαδικασίες που απαιτούνται από τον παρόντα ΚΠ, ότι το Πιστοποιητικό ΥπΑΠ εκδόθηκε για Φορέα άλλον από αυτόν που κατονομάζεται ως το Υποκείμενο του πιστοποιητικού ΥπΑΠ ή χωρίς την έγκριση αυτού.

ο Διαπιστώσει ότι δεν τηρούνται οι όροι του παρόντος κανονισμού ή υπάρχει παραίτηση από μια ουσιώδη προϋπόθεση για την Έκδοση Πιστοποιητικού ΥπΑΠ.

4.4.2. Ποιος Μπορεί να Ζητήσει Ανάκληση Πιστοποιητικού

4.4.2.1. Ποιος Μπορεί να Ζητήσει Ανάκληση Πιστοποιητικού Τελικού Χρήστη

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) ή η ΥπΑΠ δύναται να ζητήσει την ανάκληση οιουδήποτε Πιστοποιητικού Τελικού Χρήστη σύμφωνα με την § 4.4.1.1. του ΚΠ. Οι Τελικοί Χρήστες δύνανται να ζητήσουν ανάκληση των δικών τους Πιστοποιητικών.

4.4.2.2. Ποιος Μπορεί να Ζητήσει Ανάκληση Πιστοποιητικού ΥπΑΠ

Η ΑΠΕΔ ή η ΥπΑΠ έχει δικαίωμα να ζητήσει την ανάκληση πιστοποιητικού ΥπΑΠ που έχει εκδοθεί για την τελευταία, σύμφωνα με τις διατάξεις του άρθρου 20 του Ν. 3448/2006.

4.4.3. Διαδικασία για Υποβολή Αιτήματος Ανάκλησης Πιστοποιητικού

4.4.3.1. Διαδικασία για Υποβολή Αιτήματος Ανάκλησης Πιστοποιητικού Τελικού Χρήστη

Ένας Τελικός Χρήστης που επιθυμεί ανάκληση του πιστοποιητικού του πρέπει να υποβάλλει αίτημα στο αρμόδιο Εντεταλμένο Γραφείο. Το αίτημα αυτό διαβιβάζεται στην υπεύθυνη ΑΕ που έχει εγκρίνει την Ηλεκτρονική Εγγραφή του Τελικού Χρήστη για Πιστοποιητικά και η οποία είναι αρμόδια να το ανακαλέσει άμεσα.

4.4.4. Συνθήκες για Αναστολή Πιστοποιητικού

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δεν παρέχει υπηρεσίες αναστολής για πιστοποιητικά ΥπΑΠ ή πιστοποιητικά Τελικού Χρήστη.

4.4.5. Ποιος Μπορεί να Ζητήσει Αναστολή Πιστοποιητικού

Δεν ισχύει.

4.4.6. Διαδικασία για Υποβολή Αιτήματος Αναστολής

Δεν ισχύει.

4.4.7. Περιορισμοί για το Χρονικό Διάστημα Αναστολής

Δεν ισχύει.

4.4.8. Συχνότητα Έκδοσης Καταλόγου Ανακληθέντων Πιστοποιητικών (ΚΑΠ)

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δημοσιεύει ΚΑΠ όπου εμπεριέχονται τα Πιστοποιητικά που έχουν ανακληθεί από την ίδια και προσφέρει παράλληλα υπηρεσίες ελέγχου κατάστασης Πιστοποιητικών. Οι ΚΑΠ για πιστοποιητικά που εκδίδει η ΑΠΕΔ δημοσιεύονται κάθε τρίμηνο, καθώς επίσης και κάθε φορά που ανακαλείται κάποιο Πιστοποιητικό. Οι ΚΑΠ για πιστοποιητικά που εκδίδουν οι ΥπΑΠ δημοσιεύονται καθημερινά. Τα Πιστοποιητικά που έχουν λήξει αφαιρούνται από τους ΚΑΠ το αργότερο τριάντα (30) ημέρες μετά από τη λήξη τους.

4.4.9. Απαιτήσεις Ελέγχου Καταλόγου Ανακληθέντων Πιστοποιητικών

Οι Τρίτοι Συμμετέχοντες θα πρέπει να ελέγχουν την κατάσταση των Πιστοποιητικών στα οποία επιθυμούν να βασιστούν, ανατρέχοντας στον πιο πρόσφατο ΚΑΠ που δημοσιεύτηκε από την ΑΠΕΔ ή την ΥπΑΠ που εξέδωσε το Πιστοποιητικό εκείνο, στο οποίο ο Τρίτος Συμμετέχων επιθυμεί να βασιστεί.

Για την Πρωτεύουσα Αρχή Πιστοποίησης (ΑΠΕΔ) και τις ΥπΑΠ, οι ΚΑΠ παρατίθενται στο χώρο αποθήκευσης αυτών στη διεύθυνση: http://www.syzefxis.gov.gr. Επιπλέον ένας «Πίνακας αναφοράς ΚΑΠ» ανακοινώνεται στο Χώρο Αποθήκευσης στη διεύθυνση: http://www.syzefxis.gov.gr, ώστε να επιτρέπει στους Τρίτους Συμμετέχοντες να προσδιορίσουν για κάθε ΥπΑΠ την ακριβή τοποθεσία αποθήκευσης του ΚΑΠ.

4.4.10. Διαθεσιμότητα Δικτυακού Ελέγχου Ανάκλησης/Κατάστασης Πιστοποιητικών

Πλέον της δημοσίευσης ΚΑΠ, η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) παρέχει πληροφορίες για την κατάσταση πιστοποιητικών μέσω μηχανισμών αναζήτησης στο Χώρο Αποθήκευσής της.

Οι πληροφορίες για την κατάσταση πιστοποιητικών είναι διαθέσιμες με τη χρήση διαδικτυακών μηχανισμών αναζήτησης (που είναι προσβάσιμες από το Χώρο Αποθήκευσης της ΑΠΕΔ) στη διεύθυνση: http://www.syzefxis.gov.gr

4.4.11. Απαιτήσεις Δικτυακού Ελέγχου Ανάκλησης

Κάθε Τρίτος Συμμετέχων δύναται να ελέγξει την κατάσταση ενός Πιστοποιητικού στο οποίο επιθυμεί να βασιστεί ανατρέχοντας στον πιο πρόσφατο σχετικό ΚΑΠ ή εναλλακτικά θα πρέπει να ελέγξει την κατάσταση του Πιστοποιητικού αυτού χρησιμοποιώντας μία από τις διαθέσιμες μεθόδους όπως προσδιορίζονται στην § 4.4.10. του ΚΠ.

4.4.12. Άλλες Διαθέσιμες Μορφές Αναγγελίας Ανάκλησης

Δεν προβλέπεται.

4.4.13. Απαιτήσεις Ελέγχου για Άλλες Μορφές Αναγγελιών Ανάκλησης

Δεν προβλέπεται.

4.4.14. Ειδικές Απαιτήσεις Σχετικά με την Έκθεση σε Κίνδυνο του Κλειδιού

Πλέον των διαδικασιών που περιγράφονται στις § 4.4.8 - 4.4.13 του ΚΠ, η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) καταβάλλει κάθε εύλογη προσπάθεια ώστε να ενημερώνει τους δυνητικούς Τρίτους Συμμετέχοντες με σχετική ανακοίνωση στην ηλεκτρονική διεύθυνση www.syzefxis.gov.gr στην περίπτωση που ανακαλύψει ή έχει λόγο να πιστεύει, ότι έχει υπάρξει Έκθεση σε Κίνδυνο του ιδιωτικού κλειδιού μιας ΥπΑΠ.

4.4.15. Ανάκτηση Κλειδιών Κρυπτογράφησης

Αποκλειστικά και μόνο για σύννομους σκοπούς, για να διασφαλιστεί η λειτουργικότητα της παρεχόμενης Υποδομής Δημοσίου Κλειδιού υποστηρίζεται η δυνατότητα ανάκτησης των ιδιωτικών κλειδιών των πιστοποιητικών κρυπτογράφησης.

Η ΑΠΕΔ στο πλαίσιο αυτό διασφαλίζει τα ακόλουθα:

Προστατεύει τα ιδιωτικά κλειδιά κρυπτογράφησης των τελικών χρηστών από μη-εξουσιοδοτημένη αποκάλυψη.

Ενημερώνει τους τελικούς χρήστες πως το ιδιωτικό κλειδί κρυπτογράφησης τους έχει ανακτηθεί, εφόσον λάβει χώρα η συγκεκριμένη ενέργεια.

Προστατεύει όλες τις πληροφορίες που μπορεί να χρησιμοποιηθούν για την ανάκτηση των κλειδιών που έχουν αποθηκευτεί.

Διανέμει τα ανακτημένα κλειδιά των τελικών χρηστών μόνο μετά από έγκυρα και εγκεκριμένα εξουσιοδοτημένα αιτήματα για ανάκτηση.

Ανακαλεί το ζεύγος κλειδιών κρυπτογράφησης των τελικών χρηστών πριν την ανάκτηση του αντίστοιχου ιδιωτικού κλειδιού.

Σε καμία περίπτωση δεν ανακτώνται τα ιδιωτικά κλειδιά πιστοποιητικών υπογραφής τελικών χρηστών.

4.5. Διαδικασίες Ελέγχου Ασφάλειας

4.5.1. Μορφές Συμβάντων που Καταγράφονται

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) διασφαλίζει όπου απαιτείται την καταγραφή των παρακάτω σημαντικών περιστατικών:

Περιστατικά διαχείρισης του κύκλου ζωής των κλειδιών της ΑΠΕΔ και των ΥπΑΠ, συμπεριλαμβανομένων:

● Της παραγωγής, δημιουργίας εφεδρικών αντιγράφων, αποθήκευσης, ανάκτησης, αρχειοθέτησης και καταστροφής κλειδιών και

● Περιστατικών διαχείρισης του κύκλου ζωής των συσκευών κρυπτογράφησης.

Περιστατικά διαχείρισης του κύκλου ζωής πιστοποιητικών ΥπΑΠ και Τελικών Χρηστών, συμπεριλαμβανομένων:

● «Εντύπων ΥΔΚ».

● Επιτυχούς ή μη επεξεργασίας των Ηλεκτρονικών Εγγραφών για πιστοποιητικά, ανανέωση, επαναδημιουργία κλειδιού, ανάκληση και ανάκτηση και

● Παραγωγής και έκδοσης Πιστοποιητικών και ΚΑΠ.

Περιστατικά σχετικά με την ασφάλεια, συμπεριλαμβανομένων:

● Επιτυχών ή μη προσπαθειών πρόσβασης στο σύστημα ΥΔΚ.

● Ενεργειών ΥΔΚ και συστήματος ασφάλειας.

● Αρχείων ή μητρώων υψηλής ασφάλειας που είναι διαθέσιμα προς ανάγνωση, εγγραφή ή διαγραφή.

● Μεταβολών στο επίπεδο ασφάλειας.

● Εμπλοκών του συστήματος, βλαβών του εξοπλισμού ή άλλων ανωμαλιών.

● Δραστηριότητας του συστήματος προστασίας (firewall) και δρομολογητή (router) και

● Εισόδου/ εξόδου επισκεπτών στις εγκαταστάσεις του αναδόχου του υποέργου 9 του «Σύζευξις».

Οι καταχωρίσεις αυτές περιλαμβάνουν τα ακόλουθα στοιχεία:

● Ημερομηνία και ώρα της καταχώρισης.

● Σειριακό ή αύξοντα αριθμό καταχώρισης, για αυτόματες καταχωρίσεις.

● Στοιχεία ταυτότητας του προσώπου που κάνει την καταχώριση.

● Είδος καταχώρισης.

Οι Αρχές Εγγραφής ή/και τα Εντεταλμένα Γραφεία καταγράφουν τα στοιχεία των «Εντύπων ΥΔΚ», συμπεριλαμβάνοντας:

● Το είδος των αποδεικτικών εγγράφων για την ταυτοποίηση του Τελικού Χρήστη.

● Καταγραφή μοναδικών δεδομένων ταυτότητας, αριθμών ή συνδυασμού αυτών των αποδεικτικών στοιχείων ταυτότητας (π.χ. του αριθμού ταυτότητας του Αιτούντος Πιστοποιητικό), εφόσον ισχύουν.

● Τοποθεσία αποθήκευσης αντιγράφων των «Εντύπων ΥΔΚ» και των αποδεικτικών εγγράφων ταυτότητας.

● Στοιχεία ταυτότητας του προσώπου που παραλαμβάνει το «Έντυπο ΥΔΚ».

● Μέθοδο που εφαρμόστηκε για την επιβεβαίωση των εγγράφων ταυτοποίησης, εφόσον υπάρχει.

4.5.2. Συχνότητα Επεξεργασίας των Αρχείων Καταγραφής

Τα αρχεία καταγραφής εξετάζονται τουλάχιστον σε εβδομαδιαία βάση για σημαντικά περιστατικά ασφάλειας και λειτουργίας. Επιπροσθέτως, η ΑΠΕΔ διασφαλίζει την ανασκόπηση των αρχείων καταγραφής για ύποπτη ή ασυνήθη δραστηριότητα βάσει των προειδοποιητικών μηνυμάτων που δημιουργούνται όταν υπάρχουν παρατυπίες ή προβλήματα εντός των συστημάτων της παρούσας ΥΔΚ.

4.5.3. Περίοδος Διατήρησης του Ημερολογίου Καταγραφής Ελέγχων

Τα αρχεία καταγραφής τηρούνται επιτόπια τουλάχιστον για δύο (2) μήνες μετά από την επεξεργασία τους, ενώ στη συνέχεια αρχειοθετούνται σύμφωνα με την § 4.6.2 του ΚΠ.

4.5.4. Προστασία του Αρχείου Καταγραφής

Τα ηλεκτρονικά και χειρόγραφα αρχεία καταγραφής προστατεύονται από μη-εξουσιοδοτημένη ανάγνωση, τροποποίηση, διαγραφή ή άλλη παραποίηση με τη χρήση φυσικών και λογικών μέτρων ελέγχου πρόσβασης.

4.5.5. Διαδικασίες Εφεδρικών Αντιγράφων των Αρχείων Καταγραφής

Εφεδρικά αντίγραφα προσθήκης (incremental backups) στα αρχεία καταγραφής δημιουργούνται καθημερινά, ενώ πλήρη εφεδρικά αντίγραφα παράγονται εβδομαδιαίως (full backups).

4.5.6. Σύστημα Ελέγχου

Αυτοματοποιημένα δεδομένα ελέγχου παράγονται και καταγράφονται σε επίπεδο εφαρμογής, δικτύου και λειτουργικού συστήματος.

4.5.7. Αξιολόγηση Τρωτών Σημείων

Τα περιστατικά που λαμβάνουν χώρα κατά τη διαδικασία ελέγχου καταγράφονται, ώστε να είναι δυνατή η παρακολούθηση των τρωτών σημείων του συστήματος. Αξιολογήσεις για την τρωτότητα της λογικής ασφάλειας («ΑΤΛΑ») (Αξιολόγηση Τρωτότητας Λογικής Ασφάλειας) διενεργούνται, ανασκοπούνται και αναθεωρούνται μετά από εξέταση των περιστατικών που έχουν καταγραφεί. Οι ΑΤΛΑ βασίζονται σε δεδομένα αυτοματοποιημένης καταγραφής πραγματικού χρόνου και διενεργούνται σε καθημερινή, μηνιαία και ετήσια βάση. Η ετήσια ΑΤΛΑ αποτελεί στοιχείο αναφοράς για τον ετήσιο Έλεγχο Συμμόρφωσης.

4.6. Καταγραφή Αρχείων

4.6.1. Είδη Περιστατικών που Καταγράφονται

Πλέον των αρχείων ελέγχου καταγραφής για λόγους ασφάλειας που προσδιορίζονται στην § 4.5 του ΚΠ, η Αρχή Πιστοποίηση Ελληνικού (ΑΠΕΔ) διασφαλίζει την τήρηση αρχείων που περιλαμβάνουν τεκμηρίωση των ακόλουθων:

● Της συμμόρφωσης με τον ΚΠ και τις υποχρεώσεις που απορρέουν από τους ΟΧΠ Τελικού Χρήστη.

● Ενεργειών και πληροφοριών που είναι ουσιώδεις για την έκδοση κάθε Πιστοποιητικού καθώς και για τη δημιουργία, έκδοση, ανάκληση, λήξη και επαναδημιουργία κλειδιού ή ανανέωση όλων των Πιστοποιητικών που εκδίδονται.

● Των "Εντύπων ΥΔΚ" και των έγγραφων ταυτοποίησης και

● Κάθε μεταβολής που έχει επέλθει στους ΟΧΠ.

Τα αρχεία του κύκλου ζωής πιστοποιητικών που τηρούνται από τις ΥπΑΠ περιλαμβάνουν:

● Την ταυτότητα του Τελικού Χρήστη που κατονομάζεται σε κάθε Πιστοποιητικό.

● Την ταυτότητα του προσώπου που αιτείται την ανάκληση ή ανάκτηση Πιστοποιητικού.

● Άλλα πραγματικά στοιχεία που δηλώνονται στο Πιστοποιητικό.

● Ορισμένα ουσιώδη στοιχεία τα οποία σχετίζονται με την έκδοση Πιστοποιητικών, συμπεριλαμβανομένων ενδεικτικά των πληροφοριών σχετικά με την επιτυχή ολοκλήρωση του Ελέγχου Συμμόρφωσης σύμφωνα με την § 2.7 του ΚΠ.

Τα αρχεία, αναφορικά με την ταυτότητα των τελικών χρηστών που τηρούν οι ΥπΑΠ περιλαμβάνουν:

● Τα είδη των εγγράφων που προσκομίζονται από τους Τελικούς Χρήστες σύμφωνα με το «Έντυπο ΥΔΚ».

● Ένα αρχείο μοναδικών στοιχείων ταυτοποίησης (πχ. αριθμός ταυτότητας, διαβατηρίου του Τελικού Χρήστη).

● Τα στοιχεία ταυτότητας του προσώπου που λαμβάνει και αποδέχεται Ηλεκτρονικές Αιτήσεις για Πιστοποιητικά και

● Ένα σχέδιο τεκμηρίωσης αναφορικά με τις μεθόδους που χρησιμοποιούνται για την αποδοχή εγγράφων ταυτοποίησης.

Τα αρχεία μπορεί να τηρούνται ηλεκτρονικά ή σε τυπωμένη μορφή, υπό την προϋπόθεση ότι έχουν ταξινομηθεί, αποθηκευθεί, τηρηθεί και αναπαραχθεί με ακρίβεια στο σύνολό τους.

4.6.2. Περίοδος Διατήρησης Αρχείου

Τα αρχεία που συνδέονται με κάποιο Πιστοποιητικό, καθώς και τα ίδια τα πιστοποιητικά διατηρούνται τουλάχιστον για τριάντα (30) έτη, μετά από την ημερομηνία λήξης ή ανάκλησης του Πιστοποιητικού

4.6.3. Προστασία του Αρχείου

Η ΑΠΕΔ διασφαλίζει την προστασία των αρχείων που καταγράφονται σύμφωνα με την § 4.6.1 του ΚΠ, με τρόπο ώστε μόνο εξουσιοδοτημένα πρόσωπα να επιτρέπεται να έχουν πρόσβαση σε αυτά. Τα ηλεκτρονικά αρχειοθετημένα δεδομένα προστατεύονται έναντι μη-εξουσιοδοτημένης ανάγνωσης, τροποποίησης, διαγραφής ή άλλης παραποίησης με την εφαρμογή κατάλληλων φυσικών και λογικών μέτρων ελέγχου πρόσβασης. Τα μέσα τήρησης των δεδομένων που αρχειοθετούνται, καθώς και οι απαιτούμενες εφαρμογές για την επεξεργασία των δεδομένων αυτών διατηρούνται, με σκοπό να διασφαλιστεί η δυνατότητα προσπέλασης τους, για το χρονικό διάστημα που προσδιορίζεται στην § 4.6.2 του ΚΠ.

4.6.4. Διαδικασίες Αρχειοθέτησης Εφεδρικών Αντιγράφων

Η ΑΠΕΔ μέσω των υποδομών του αναδόχου του υποέργου 9 του έργου Σύζευξις δημιουργεί σε καθημερινή βάση εφεδρικά αντίγραφα (back-up) των στοιχείων που υπάρχουν στα εκδοθέντα πιστοποιητικά μέσω της αποθήκευσης των επιπρόσθετων πληροφοριών (incremental back up), ενώ παράγει πλήρη εφεδρικά αντίγραφα (full back up) σε εβδομαδιαία βάση.

4.6.5. Απαιτήσεις για τη Χρονοσήμανση των Αρχείων

Δεν ισχύει.

4.6.6. Διαδικασίες για την Πρόσβαση και την Επαλήθευση Πληροφοριών Αρχείου

Βλ. ΚΠ § 4.6.3.

4.7. Αντικατάσταση Κλειδιών

Τα ζεύγη κλειδιών που πιστοποιούν τις ΥπΑΠ αποσύρονται με το πέρας του αντίστοιχου ανώτατου χρόνου ζωής τους όπως ορίζεται στην § 6.3.2 του ΚΠ.

Πριν από τη λήξη των πιστοποιητικών που πιστοποιούν τις ΥπΑΠ, εφαρμόζονται διαδικασίες αντικατάστασης των κλειδιών. Η διαδικασία αντικατάστασης κλειδιών που πιστοποιούν τις ΥπΑΠ προϋποθέτει ότι:

● Η ΥπΑΠ διακόπτει την έκδοση νέων πιστοποιητικών όχι αργότερα από 60 ημέρες πριν από την ημερομηνία λήξεως του ζεύγους των κλειδιών της.

● Τα πιστοποιητικά τελικών χρηστών μετά την επαναδημιουργία του ζεύγους κλειδιών που πιστοποιούν τις ΥπΑΠ θα υπογράφονται από το νέο ζεύγος κλειδιών της ΥπΑΠ.

● Η ΥπΑΠ θα συνεχίζει να εκδίδει ΚΑΠ υπογεγραμμένους από το αρχικό ιδιωτικό κλειδί της μέχρι την επέλευση της ημερομηνίας λήξεως του τελευταίου Πιστοποιητικού που εκδόθηκε με τη χρήση αυτού του αρχικού ζεύγους κλειδιών.

4.8. Αποκατάσταση Καταστροφών και Έκθεσης σε Κίνδυνο του Κλειδιού

Η ΑΠΕΔ διασφαλίζει μέσω των υποδομών του αναδόχου του υποέργου 9 του έργου Σύζευξις την υλοποίηση ενός ισχυρού συνδυασμού φυσικών, λογικών και διαδικαστικών μέτρων ελέγχου ώστε να ελαχιστοποιήσει τον κίνδυνο και τον πιθανό αντίκτυπο της Έκθεσης σε Κίνδυνο ή της καταστροφής κάποιου κλειδιού. Επιπρόσθετα, εφαρμόζονται μέτρα αποκατάστασης καταστροφών όπως περιγράφεται στην § 4.8.2 του ΚΠ και μέτρα αντιμετώπισης της Έκθεσης Κλειδιού σε Κίνδυνο όπως περιγράφεται στην § 4.8.3 ΚΠ. Τα μέτρα που αναπτύσσονται για την αποκατάσταση Έκθεσης σε Κίνδυνο ή καταστροφής αναπτύσσονται με στόχο την ελαχιστοποίηση του πιθανού αντίκτυπου από τέτοιο συμβάν και την αποκατάσταση της λειτουργίας της ΥΔΚ.

4.8.1. Φθορά Εξοπλισμού, Λογισμικού, Δεδομένων

Σε περίπτωση φθοράς του εξοπλισμού, λογισμικού ή/και δεδομένων εφαρμόζονται τα μέτρα αντιμετώπισης επεισοδίων. Τα μέτρα αυτά απαιτούν ανάλογη κλιμάκωση, διερεύνηση του επεισοδίου και ανταπόκριση στο επεισόδιο. Τα μέτρα για την αποκατάσταση καταστροφής ή έκθεσης σε κίνδυνο του κλειδιού θα τεθούν σε ισχύ εφόσον κριθεί απαραίτητο.

4.8.2. Αποκατάσταση Καταστροφών

Δημιουργούνται εφεδρικά αρχεία για τα κρίσιμα στοιχεία της ΑΠΕΔ και των ΥπΑΠ της παρούσας ΥΔΚ, τόσο εξοπλισμού όσο και λογισμικού. Επιπλέον, λαμβάνονται αντίγραφα των ιδιωτικών κλειδιών της ΑΠΕΔ και των ΥπΑΠ με σκοπό την αποκατάσταση από καταστροφή.

Επίσης, αναπτύσσονται μέτρα εφαρμογής ενός σχεδίου αποκατάστασης από καταστροφή. Στο σχέδιο αυτό περιλαμβάνεται η ύπαρξη χώρου αποκατάστασης από καταστροφή ώστε να ελαχιστοποιηθούν οι συνέπειες οιασδήποτε φυσικής ή άλλης καταστροφής. Η παραπάνω στρατηγική αναθεωρείται τακτικά, ελέγχεται και ενημερώνεται για να είναι λειτουργική σε περίπτωση καταστροφής. Τα μέτρα αυτά είναι σε θέση να επιτύχουν αποκατάσταση των πληροφοριακών συστημάτων και των βασικών επιχειρησιακών λειτουργιών.

Τέλος, διατηρούνται αντίγραφα σε άλλο χώρο (Disaster recovery site) των σημαντικών πληροφοριών της ΑΠΕΔ και των ΥπΑΠ. Τέτοιες πληροφορίες περιλαμβάνουν ιδίως, αρχεία καταγραφής των συστημάτων και των εφαρμογών, στοιχεία του «Εντύπου ΥΔΚ», στοιχεία ελέγχου, καθώς και τα αρχεία βάσεων δεδομένων για όλα τα πιστοποιητικά που εκδίδονται.

4.8.3. Έκθεση σε Κίνδυνο

Κατά την υποτιθέμενη ή πραγματική Έκθεση σε Κίνδυνο του ιδιωτικού κλειδιού της ΑΠΕΔ ή των ΥπΑΠ, εφαρμόζονται ειδικά μέτρα για την Αντιμετώπιση της

Έκθεσης Κλειδιού σε Κίνδυνο από την Ομάδα Αντιμετώπισης Επεισοδίων και Έκθεσης σε Κίνδυνο (ΟΑΕΕΚ) (Compromise Incident Response Team) του αναδόχου του υποέργου 9 του έργου «Σύζευξις» ή του φορέα που θα αναλάβει τη διαχείριση της Υποδομής Δημοσίου Κλειδιού. Η ομάδα αυτή, αξιολογεί την κατάσταση, αναπτύσσει σχέδιο δράσης και εκτελεί το σχέδιο αυτό με την έγκριση της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ).

Εφόσον απαιτείται ανάκληση Πιστοποιητικού ΑΠ, λαμβάνονται τα ακόλουθα μέτρα:

- Η κατάσταση ανάκλησης του Πιστοποιητικού κοινοποιείται στους Τρίτους Συμμετέχοντες μέσω του Χώρου Αποθήκευσης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) σύμφωνα με την § 4.4.9 του ΚΠ.
- Καταβάλλεται εύλογη προσπάθεια ώστε να υπάρξει πρόσθετη ενημέρωση σχετικά με την ανάκληση προς όλους τους Συμμετέχοντες που δύναται να επηρεαστούν.
- Η ΑΠ θα παράγει ένα νέο ζεύγος κλειδιών σύμφωνα με την § 4.7 του ΚΠ, εκτός της περίπτωσης όπου διακόπτεται η παροχή των υπηρεσιών πιστοποίησης σύμφωνα με την§ 4.9 του ΚΠ.

4.9. Διακοπή Παροχής των Υπηρεσιών μιας ΑΠ

Στην περίπτωση που είναι απαραίτητη η διακοπή παροχής των υπηρεσιών πιστοποίησης της ΑΠΕΔ ή μιας ΥπΑΠ, η εν λόγω ΑΠ υποχρεούται με κάθε πρόσφορο μέσο να ενημερώσει όσους επηρεάζονται άμεσα από την εν λόγω διακοπή, τους Τελικούς Χρήστες, Τρίτους Συμμετέχοντες κ.α. για τη διακοπή παροχής των υπηρεσιών της (πιστοποίησης) πριν αυτή επέλθει, με σχετική ανακοίνωσή της στην ηλεκτρονική διεύθυνση www.syzefxis.gov.gr.

Ενόψει της διακοπής παροχής των υπηρεσιών πιστοποίησης της ΑΠΕΔ ή μιας ΥπΑΠ σύμφωνα με τα παραπάνω, αναπτύσσεται από την εν λόγω ΑΠ σχέδιο δράσης το οποίο δύναται να περιλαμβάνει κατ' ελάχιστο, τα ακόλουθα:

- Αναγγελία στους φορείς ή τα πρόσωπα που επηρεάζονται από τη διακοπή των υπηρεσιών πιστοποίησης , όπως είναι οι Τελικοί Χρήστες, οι Τρίτοι Συμμετέχοντες κ.α..
- Ανάκληση του Πιστοποιητικού ΥπΑΠ που εκδόθηκε από την ΑΠΕΔ (σε περίπτωση που διακόπτει τις υπηρεσίες πιστοποίησης μια ΥπΑΠ).
- Διατήρηση των αρχείων και των εγγράφων της ΑΠ για τα χρονικά διαστήματα που απαιτούνται από την § 4.6.2 του ΚΠ, περιλαμβανομένων και των υποχρεώσεων του αναδόχου του υποέργου 9 του έργου ΣΥΖΕΥΞΙΣ.
- Συνεχή και αδιάκοπη παροχή των υπηρεσιών υποστήριξης του Τελικού Χρήστη.
- Συνεχή παροχή των υπηρεσιών ανάκλησης, όπως είναι η έκδοση ΚΑΠ ή η υποστήριξη υπηρεσιών δικτυακού ελέγχου κατάστασης Πιστοποιητικών.
- Ανάκληση των Πιστοποιητικών Τελικών Χρηστών τα οποία δεν έχουν λήξει ή ανακληθεί, εφόσον είναι απαραίτητο.
- Προϋποθέσεις διάθεσης του ιδιωτικού κλειδιού της ΑΠ και των Ασφαλών Κρυπτογραφικών Μονάδων που περιλαμβάνουν αυτό το ιδιωτικό κλειδί με ασφαλή μέσα.

4.9.1. Διαχείριση των αρχείων σε περίπτωση διακοπής των υπηρεσιών πιστοποίησης



Η τήρηση και η επεξεργασία των αρχείων προσωπικών δεδομένων που τηρούνται από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και τις ΥπΑΠ λαμβάνει χώρα σύμφωνα με τα οριζόμενα στην ισχύουσα νομοθεσία για την προστασία των προσωπικών δεδομένων. Τα συγκεκριμένα αρχεία διατηρούνται για χρονική περίοδο τριάντα (30) ετών.

5. Φυσικά, Διαδικαστικά Μέτρα Προστασίας και Ασφάλειας Προσωπικού

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ), μέσω των υποδομών του αναδόχου του υποέργου 9 του έργου «ΣΥΖΕΥΞΙΣ», εφαρμόζει υψηλές προδιαγραφές ασφαλείας οι οποίες ανταποκρίνονται στον παρόντα ΚΠ.

5.1. Φυσικά Μέτρα Προστασίας

5.1.1. Χώρος Εγκατάστασης και Κατασκευή

Οι υπηρεσίες πιστοποίησης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και των ΥπΑΠ διενεργούνται μέσω των υποδομών του αναδόχου του υποέργου 9 του έργου «Σύζευξις» εντός φυσικά προστατευμένου περιβάλλοντος το οποίο έχει σχεδιαστεί έτσι ώστε να αποτρέπεται, να προλαμβάνεται και να εντοπίζεται κάθε εμφανής ή μη προσπάθεια πρόσβασης, ικανοποιώντας τους διεθνώς αναγνωρισμένους, βάσει προτύπων, όρους και προϋποθέσεις ασφαλείας.

5.1.2. Φυσική Πρόσβαση

Για να επιτευχθεί πρόσβαση σε κάποιο ανώτερο επίπεδο πρόσβασης απαιτείται να επιτραπεί η είσοδος καταρχήν σε κάποιο κατώτερο επίπεδο πρόσβασης. Ειδικότερα υπάρχουν επίπεδα πρόσβασης που περιλαμβάνουν :

- Κοινόχρηστους χώρους
- Επίπεδο στο οποίο λαμβάνει χώρα η ευαίσθητη λειτουργική δραστηριότητα των ΑΠ.
- Χώρο αποθήκευσης των Ασφαλών Κρυπτογραφικών Μονάδων (ΑΚΜ).

5.1.3. Παροχή Ηλεκτρικού Ρεύματος και Κλιματισμός

Οι ασφαλείς εγκαταστάσεις των υποδομών μέσω των οποίων παρέχονται οι υπηρεσίες πιστοποίησης βάσει των διατάξεων του παρόντος και τις συναφθείσες συμβάσεις, είναι εξοπλισμένες με κύρια και εφεδρικά:

- Συστήματα παροχής ηλεκτρικού ρεύματος για την εξασφάλιση συνεχούς και αδιάλειπτης παροχής.
- Συστήματα θέρμανσης/ εξαερισμού/ κλιματισμού για τον έλεγχο της θερμοκρασίας και της σχετικής υγρασίας.

5.1.4. Πλημμύρες

Λαμβάνονται οι απαιτούμενες προφυλάξεις για να ελαχιστοποιηθούν οι κίνδυνοι από πλημμύρες.

5.1.5. Πρόληψη και Προστασία από Φωτιά

Λαμβάνονται όλες οι απαραίτητες προφυλάξεις για την πρόληψη και κατάσβεση πυρκαγιάς ή άλλης επιζήμιας έκθεσης σε φωτιά ή καπνό. Τα μέτρα αυτά έχουν σχεδιαστεί ώστε να πληρούν τους εθνικούς κανονισμούς ασφάλειας από φωτιά.

5.1.6. Αποθήκευση Μέσων

Όλα τα μέσα τα οποία περιέχουν το λογισμικό και τα δεδομένα παραγωγής, καθώς και τα στοιχεία ελέγχων, αρχείου ή εφεδρικών αντιγράφων αποθηκεύονται σε ασφαλείς εγκαταστάσεις αποθήκευσης οι οποίες διαθέτουν τα απαραίτητα φυσικά και λογικά μέτρα ελέγχου πρόσβασης. Τα μέτρα αυτά σχεδιάζονται ώστε να περιορίζουν την πρόσβαση αποκλειστικά σε εξουσιοδοτημένο προσωπικό και να προστατεύουν τα μέσα αποθήκευσης

έναντι οιασδήποτε καταστροφής (π.χ., από νερό, φωτιά ή/και ηλεκτρομαγνητική).

5.1.7. Καταστροφή Μη-Χρήσιμων Υλικών

Τα διαβαθμισμένα έγγραφα και υλικά καταστρέφονται σε καταστροφέα εγγράφων και τα μέσα που χρησιμοποιήθηκαν για τη συλλογή ή μεταβίβαση διαβαθμισμένων πληροφοριών καθίστανται μη-αναγνώσιμα. Οι συσκευές κρυπτογράφησης καταστρέφονται με φυσικό τρόπο ή διαγράφονται τα δεδομένα τους σύμφωνα με τις οδηγίες του κατασκευαστή. Τα υπόλοιπα μη-χρήσιμα υλικά καταστρέφονται.

5.1.8. Δημιουργία Εφεδρικών Αντιγράφων Ασφαλείας Εκτός του Κύριου Χώρου

Ανά τακτά διαστήματα δημιουργούνται εφεδρικά αντίγραφα για τα δεδομένα των κυριότερων συστημάτων, των δεδομένων καταχώρισης ελέγχου, καθώς και άλλων διαβαθμισμένων πληροφοριών.

5.1.9. Υλικοτεχνική υποδομή

Όλη η υποδομή βάσει της οποίας παρέχονται οι υπηρεσίες πιστοποίησης σύμφωνα με τις διατάξεις του παρόντος και τις συναφθείσες συμβάσεις, διαχωρίζεται σε δύο επίπεδα λειτουργίας, τη δοκιμαστική (staging) και την κανονική (production) όπου η δοκιμαστική υποδομή λειτουργίας αποτελεί ένα πιστό αντίγραφο της κανονικής υποδομής. Τα επιμέρους συστατικά που απαρτίζουν την παραπάνω υποδομή αποτελούνται μεταξύ άλλων από μια σειρά από εξυπηρετητές οι οποίοι επιτελούν κρίσιμες λειτουργίες όπως:

- Την αποθήκευση όλων των πληροφοριών που αφορούν τις Ηλεκτρονικές Αιτήσεις για πιστοποιητικά, εγκρίσεις πιστοποιητικών, ανακλήσεις και άλλα στοιχεία.
- Την επεξεργασία δεδομένων εισόδου, όπως οι αιτήσεις εγγραφής πιστοποιητικών και οι αιτήσεις ανεύρεσης στοιχείων από τη βάση δεδομένων.
- Τη διατήρηση των κλειδιών των Αρχών Πιστοποίησης και την ψηφιακή υπογραφή των πιστοποιητικών των χρηστών ανάλογα με την Αρχή Πιστοποίησης, χρησιμοποιώντας Ασφαλείς Κρυπτογραφικές Μονάδες που καλύπτουν την προδιαγραφή Common Criteria Evaluation Assurance Level 4 (CC EAL4) σύμφωνα με την κείμενη εθνική νομοθεσία.
- Τον έλεγχο σε τακτά χρονικά διαστήματα όλων των λειτουργιών και ενημέρωση των υπευθύνων για τυχόν προβλήματα.

Επίσης χρησιμοποιείται επαρκής εξοπλισμός για την προστασία της περιμετρικής και εσωτερικής ασφάλειας του δικτύου από κακόβουλες επιθέσεις, είτε εξωτερικές είτε εσωτερικές, την ανίχνευση επιθέσεων σε επίπεδο εφαρμογής και για τον διαμοιρασμό της δικτυακής κίνησης.

5.2. Διαδικαστικά Μέτρα Ελέγχου

5.2.1. Έμπιστοι Ρόλοι

Ως Έμπιστα Πρόσωπα θεωρούνται όλοι οι υπάλληλοι, εργολήπτες και σύμβουλοι οι οποίοι έχουν πρόσβαση ή ελέγχουν λειτουργίες ταυτοποίησης ή κρυπτογράφησης και οι οποίοι θα μπορούσαν να επηρεάσουν σημαντικά:

- Την εγκυρότητα των στοιχείων στα "Έντυπα ΥΔΚ" και στην Ηλεκτρονική Εγγραφή για πιστοποιητικά.
- Την αποδοχή, απόρριψη ή άλλη επεξεργασία των ηλεκτρονικών αιτήσεων για πιστοποιητικά, των αιτημάτων για ανάκληση ή των αιτημάτων για ανανέωση ή των στοιχείων εγγραφής.
- Την έκδοση ή ανάκληση Πιστοποιητικών, περιλαμβανομένου του προσωπικού που έχει πρόσβαση στις περιοχές περιορισμένης πρόσβασης στο χώρο αποθήκευσης.
- Τον χειρισμό των στοιχείων ή των αιτημάτων των Τελικών χρηστών.

5.2.2. Απαιτήσεις Εκπαίδευσης

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και οι ΥπΑΠ, διασφαλίζουν στο προσωπικό τους, την απαραίτητη εκπαίδευση για την εκτέλεση των καθηκόντων τους με επαρκή και ικανοποιητικό τρόπο. Επίσης περιοδικά αναθεωρούν και βελτιώνουν τα εκπαιδευτικά τους προγράμματα ανάλογα με τις ανάγκες τους.

5.2.3. Συχνότητα και Απαιτήσεις Επανεκπαίδευσης

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και οι ΥπΑΠ διασφαλίζουν τη συνεχή εκπαίδευση και ενημέρωση για τις σύγχρονες εξελίξεις στο προσωπικό τους στο βαθμό και τη συχνότητα που είναι απαραίτητα ώστε να εξασφαλιστεί η διατήρηση του απαιτούμενου επιπέδου επάρκειας γνώσεων. Επίσης σε συνεχή βάση παρέχεται ενημέρωση αναφορικά με θέματα ασφαλείας.

5.2.4. Συχνότητα και Σειρά για Διαδοχή Θέσεων

Δεν προβλέπεται.

5.2.5. Έντυπα που Διατίθενται στο Προσωπικό

Το προσωπικό που αναλαμβάνει την εφαρμογή των υπηρεσιών πιστοποίησης της ΥΔΚ βάσει των διατάξεων του παρόντος, είναι σκόπιμο να λάβει πλήρη γνώση αυτού του Κανονισμού, για την άρτια εκτέλεση των καθηκόντων του. Η ΑΠΕΔ και οι ΥπΑΠ παρέχουν στους υπαλλήλους τους τα απαιτούμενα εκπαιδευτικά και άλλα έντυπα που είναι απαραίτητα για την εκτέλεση των καθηκόντων τους.

6. Τεχνικά Μέτρα Ασφαλείας

6.1. Παραγωγή και Εγκατάσταση Ζεύγους Κλειδιών

6.1.1. Παραγωγή Ζεύγους Κλειδιών

Η παραγωγή ζεύγους κλειδιών ΑΠ διενεργείται από εκπαιδευμένα και έμπιστα πρόσωπα που χρησιμοποιούν Αξιόπιστα Συστήματα και διαδικασίες οι οποίες εγγυώνται την ασφάλεια και την απαραίτητη κρυπτογραφική ισχύ για τα παραγόμενα κλειδιά. Για την Πρωτεύουσα Αρχή Πιστοποίησης (ΑΠΕΔ) και τις ΥπΑΠ , οι κρυπτογραφικές μονάδες που χρησιμοποιούνται για την παραγωγή κλειδιών πληρούν τις προδιαγραφές CC EAL 4.

Η παραγωγή ζεύγους κλειδιών υπογραφής τόσο για τον Υπεύθυνο Αρχής Εγγραφής όσο και για τους Τελικούς Χρήστες διενεργείται με τη χρήση ΑΔΔΥ (Ασφαλής Διάταξη Δημιουργίας Υπογραφής) η οποία ακολουθεί τα κριτήρια του παραρτήματος ΙΙΙ του Π.Δ. 150/2001. Ειδικότερα, κατά τη διαδικασία της Ηλεκτρονικής Εγγραφής για πιστοποιητικά:

- Δημιουργείται ένα ζεύγος δημόσιου - ιδιωτικού κλειδιού υπογραφής μέσα στην έξυπνη κάρτα-ΑΔΔΥ του τελικού χρήστη.
- Το ιδιωτικό κλειδί υπογραφής παραμένει στην έξυπνη κάρτα-ΑΔΔΥ.
- Αποστέλλεται στην Αρχή Πιστοποίησης για να υπογραφεί το δημόσιο κλειδί υπογραφής.
- Το ιδιωτικό - δημόσιο κλειδί κρυπτογράφησης δημιουργείται κεντρικά.

● Η Αρχή Πιστοποίησης επιστρέφει στον Τελικό Χρήστη τα δύο υπογεγραμμένα δημόσια κλειδιά (υπογραφής και κρυπτογράφησης), μαζί με το ιδιωτικό κλειδί κρυπτογράφησης που δημιουργήθηκε κεντρικοποιημένα και όλα μαζί αποθηκεύονται στην έξυπνη κάρτα-ΑΔΔΥ.

6.1.2. Παράδοση Ιδιωτικού Κλειδιού

Το ζεύγος κλειδιών υπογραφής (ΠΠ 1) Τελικού Χρήστη παράγεται από τον Τελικό Χρήστη. Ως εκ τούτου, σε αυτή την περίπτωση δεν υφίσταται παράδοση του ιδιωτικού κλειδιού στον Τελικό Χρήστη.

Το ζεύγος κλειδιών κρυπτογράφησης (ΠΠ 2) Τελικού Χρήστη παράγεται κεντρικοποιημένα και συνεπώς το ιδιωτικό κλειδί κρυπτογράφησης παραδίδεται στο τελικό χρήστη μέσω ασφαλούς συνδέσεως SSL (Secure Socket Layer -Επιπέδου Ασφαλών Συνδέσεων).

6.1.3. Παράδοση Δημόσιου Κλειδιού στον Εκδότη του Πιστοποιητικού

Οι Τελικοί Χρήστες υποβάλλουν ηλεκτρονικά το δημόσιο κλειδί υπογραφής τους (ΠΠ 1) στην ΥπΑΠ που θα παράσχει τις υπηρεσίες πιστοποίησης, με τη χρήση ηλεκτρονικού αιτήματος υπογραφής πιστοποιητικού (ΑΥΠ / CSR), PKCS # 10 ή άλλης ηλεκτρονικά υπογεγραμμένης μορφής, μέσω ασφαλούς συνδέσεως SSL (Secure Socket Layer -Επιπέδου Ασφαλών Συνδέσεων).

6.1.4. Παράδοση Δημόσιου Κλειδιού ΑΠ σε Χρήστες

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) καθιστά διαθέσιμα τα Πιστοποιητικά των ΥπΑΠ στους Τελικούς Χρήστες και τους Τρίτους Συμμετέχοντες από το χώρο αποθήκευσής της.

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) καθιστά διαθέσιμη την πλήρη αλυσίδα πιστοποιητικών (περιλαμβανομένων των πιστοποιητικών που εκδόθηκαν από την ΑΠΕΔ για τις ΥπΑΠ) στον Τελικό Χρήστη κατά την έκδοση ενός Πιστοποιητικού. Τα Πιστοποιητικά ΑΠ της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) μπορούν επίσης να «φορτωθούν» από Κατάλογο Lightweight Directory Access Protocol (LDAP).

6.1.5. Μέγεθος Κλειδιού

Τα ζεύγη κλειδιών της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και των ΥπΑΠ είναι 2048 bit RSA. Τα ζεύγη κλειδιών των Τελικών Χρηστών ορίζονται στα 1024 bit RSA.

6.1.6. Παραγωγή Παραμέτρων Δημόσιου Κλειδιού

Δεν ισχύει.

6.1.7. Έλεγχος Ποιότητας Παραμέτρου

Δεν ισχύει.

6.1.8. Παραγωγή Κλειδιών σε Εξοπλισμό / Λογισμικό

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) παράγει ζεύγη κλειδιών των δικών της ΑΠ σε Ασφαλείς Κρυπτογραφικές Μονάδες σύμφωνα με την § 6.2.1 του ΚΠ. Τα ζεύγη κλειδιών υπογραφής (ΠΠ 1) Τελικού Χρήστη παράγονται σε εξοπλισμό (hardware) ο οποίος πληροί τις προϋποθέσεις του παραρτήματος ΙΙΙ του ΠΔ 150/2001.

6.1.8.1. Παραγωγή Κλειδιών σε Ασφαλή Διάταξη Δημιουργίας Υπογραφής

Οι Τελικοί Χρήστες δημιουργούν τα ιδιωτικά κλειδιά των πιστοποιητικών υπογραφής τους (ΠΠ 1), κάνοντας χρήση Ασφαλούς Διάταξης Δημιουργίας Υπογραφής (ΑΔΔΥ).

6.1.9. Σκοποί της Χρήσης Κλειδιού Πιστοποιητικού

Βλ. ΚΠ § 7.1.2.1

6.2. Προστασία Ιδιωτικού Κλειδιού

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) μέσω των υποδομών του αναδόχου του υποέργου 9 του έργου «Σύζευξις» διασφαλίζει την εφαρμογή συνδυασμού φυσικών, λογικών και διαδικαστικών μέτρων τα οποία εγγυώνται την ασφάλεια των ιδιωτικών κλειδιών των ΑΠ της. Τα φυσικά μέτρα ελέγχου πρόσβασης περιγράφονται στην § 5.1.2 του ΚΠ. Οι Τελικοί Χρήστες απαιτείται να λαμβάνουν τις απαραίτητες προφυλάξεις ώστε να αποτρέψουν την απώλεια, αποκάλυψη, τροποποίηση ή μηεξουσιοδοτημένη χρήση των ιδιωτικών τους κλειδιών.

6.2.1. Πρότυπα για τις Ασφαλείς Κρυπτογραφικές Μονάδες (ΑΚΜ)

Για την παραγωγή και την αποθήκευση ιδιωτικών κλειδιών της ΑΠΕΔ και των ΥπΑΠ χρησιμοποιούνται Ασφαλείς Κρυπτογραφικές Μονάδες (ΑΚΜ) οι οποίες πληρούν τις προδιαγραφές CC EAL 4.

6.2.2. Παρακαταθήκη Ιδιωτικού Κλειδιού

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δεν καταθέτει τα ιδιωτικά κλειδιά ΑΠ ή Τελικού Χρήστη σε οιοδήποτε τρίτο πρόσωπο.

6.2.3. Παραγωγή Εφεδρικού Αντιγράφου Ιδιωτικού Κλειδιού

Δημιουργούνται εφεδρικά αντίγραφα των ιδιωτικών κλειδιών ΑΠ για την περίπτωση ανάκτησης (τακτικής ή έκτακτης). Τα κλειδιά αυτά αποθηκεύονται σε κρυπτογραφημένη μορφή εντός Ασφαλών Κρυπτογραφικών Μονάδων οι οποίες πληρούν τις προδιαγραφές της § 6.2.1 του ΚΠ. Τα ιδιωτικά κλειδιά ΑΠ αντιγράφονται σε εφεδρικές Ασφαλείς Κρυπτογραφικές Μονάδες σύμφωνα με την § 6.2.5 του ΚΠ.

Οι μονάδες που περιέχουν τα εφεδρικά αντίγραφα των ιδιωτικών κλειδιών ΑΠ υπόκεινται στις προδιαγραφές της § 6.2.1 του ΚΠ. Οι μονάδες που περιέχουν αντίγραφα για την περίπτωση αποκατάστασης από καταστροφή του ιδιωτικού κλειδιού ΑΠ υπόκεινται στις προδιαγραφές της § 4.8.2 του ΚΠ.

6.2.4. Αρχειοθέτηση Ιδιωτικών Κλειδιών

Με το τέλος της περιόδου ισχύος τους τα ζεύγη κλειδιών των ΑΠ αρχειοθετούνται για χρονικό διάστημα 30 ετών στις υποδομές του αναδόχου του υποέργου 9 του έργου «Σύζευξις». Τα αρχειοθετημένα ζεύγη κλειδιών ΑΠ αποθηκεύονται με ασφαλή τρόπο με τη χρήση Ασφαλών Κρυπτογραφικών Μονάδων οι οποίες πληρούν τις προδιαγραφές της § 6.2.1 του ΚΠ. Διαδικαστικά μέτρα ελέγχου αποτρέπουν την επιστροφή των αρχειοθετημένων ζευγών κλειδιών ΑΠ σε παραγωγική χρήση. Με το πέρας του χρονικού διαστήματος αρχειοθέτησης, τα αρχειοθετημένα ιδιωτικά κλειδιά ΑΠ θα καταστραφούν με ασφαλή τρόπο και σύμφωνα με την § 6.2.8 του ΚΠ.

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δεν αρχειοθετεί αντίγραφα των ιδιωτικών κλειδιών Υπογραφής Τελικών χρηστών.

6.2.5. Καταχώρηση Ιδιωτικού Κλειδιού σε Κρυπτογραφική Μονάδα

Τα ζεύγη κλειδιών ΑΠ παράγονται σε Ασφαλείς Κρυπτογραφικές Μονάδες (ΑΚΜ) όπου δημιουργούνται αντίγραφα τους για την περίπτωση ανάκτησης (τακτικής ή έκτακτης). Η μεταφορά ενός εφεδρικού αντιγράφου ζεύγους κλειδιών ΑΠ σε άλλη ΑΚΜ γίνεται σε κρυπτογραφημένη μορφή.

6.2.6. Μέθοδος Ενεργοποίησης Ιδιωτικού Κλειδιού

Ιδιωτικά Κλειδιά Τελικού Χρήστη

Οι Τελικοί Χρήστες θα πρέπει να κάνουν χρήση των έξυπνων καρτών - Ασφαλών Διατάξεων Δημιουργίας Υπογραφής (ΑΔΔΥ) που τους έχουν χορηγηθεί προκειμένου να αποθηκεύσουν, χρησιμοποιήσουν ή ενεργοποιήσουν τα ιδιωτικά τους κλειδιά. Παράλληλα θεωρείται υποχρεωτική από τους Τελικούς Χρήστες:

- Η χρήση του συνθηματικού πρόσβασης στην έξυπνη κάρτα (PIN/Personal Identification Number ή του μυστικού αριθμού PUK/Personal Unblocking Key) στην περίπτωση απώλειας του PIN, σύμφωνα με την § 6.4.1 του ΚΠ για την εξακρίβωση της ταυτότητας τους πριν από την ενεργοποίηση του ιδιωτικού τους κλειδιού.
- Η λήψη ευλόγων μέτρων για τη φυσική προστασία του χώρου και σταθμού εργασίας τους ώστε να αποτραπεί η χρήση των ανωτέρω καθώς και των αντίστοιχων ιδιωτικών κλειδιών χωρίς την έγκριση τους.

Κατά την απενεργοποίησή τους, τα ιδιωτικά κλειδιά θα τηρούνται μόνο σε κρυπτογραφημένη μορφή.

Υπεύθυνοι Αρχών Εγγραφής (ΑΕ)

Ακολουθούνται οι διαδικασίες που αναφέρονται ανωτέρω για τους Τελικούς Χρήστες. Κατά την απενεργοποίησή τους, τα ιδιωτικά κλειδιά των υπευθύνων ΑΕ θα τηρούνται μόνο σε κρυπτογραφημένη μορφή.

6.2.7. Μέθοδος Απενεργοποίησης Ιδιωτικού Κλειδιού

Τα ιδιωτικά κλειδιά ΑΠ της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) απενεργοποιούνται με την αφαίρεσή τους από τη συσκευή ανάγνωσης.

Τα ιδιωτικά κλειδιά τελικών χρηστών καθώς και των Υπεύθυνων ΑΕ μπορούν να απενεργοποιηθούν με την αφαίρεση της έξυπνης κάρτας-ΑΔΔΥ από τη συσκευή ανάγνωσης καρτών. Σε κάθε περίπτωση, οι Υπεύθυνοι ΑΕ καθώς και οι Τελικοί Χρήστες έχουν υποχρέωση να προστατεύουν επαρκώς τα ιδιωτικά κλειδιά τους σύμφωνα με τις § 2.1.4, § 6.4.1 ΚΠ.

6.2.8. Μέθοδος Καταστροφής Ιδιωτικού Κλειδιού

Με το πέρας του λειτουργικού χρόνου ζωής μιας ΑΠ, ένα ή περισσότερα αντίγραφα του ιδιωτικού κλειδιού της ΑΠ αρχειοθετούνται σύμφωνα με την § 6.2.5 του ΚΠ. Τα υπόλοιπα αντίγραφα του ιδιωτικού κλειδιού της ΑΠ καταστρέφονται με ασφαλή τρόπο. Επιπλέον, τα αρχειοθετημένα ιδιωτικά κλειδιά της ΑΠ καταστρέφονται με ασφαλή τρόπο με το πέρας του χρονικού διαστήματος αρχειοθέτησής τους.

Όταν είναι απαραίτητο, η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) καταστρέφει τα ιδιωτικά κλειδιά ΑΠ με τρόπο που λογικά εξασφαλίζει ότι δεν θα παραμείνουν μέρη του κλειδιού αυτού τα οποία θα μπορούσαν να οδηγήσουν στην ανασύνθεση του. Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) χρησιμοποιεί τη λειτουργία διαγραφής του περιεχομένου των Ασφαλών Κρυπτογραφικών Μονάδων της καθώς και άλλα κατάλληλα μέτρα ώστε να εξασφαλίζει την πλήρη καταστροφή των ιδιωτικών κλειδιών ΑΠ. Οι ενέργειες καταστροφής κλειδιών ΑΠ καταγράφονται κατά την εκτέλεσή τους.

6.3. Άλλα Θέματα Διαχείρισης του Ζεύγους Κλειδιών

6.3.1. Αρχειοθέτηση Δημόσιου Κλειδιού

Από τα Πιστοποιητικά ΑΠ και τελικών χρηστών της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δημιουργούνται αντίγραφα ασφαλείας τα οποία αρχειοθετούνται ως μέρος της τακτικής διαδικασίας δημιουργίας αντιγράφων μέσω των υποδομών του αναδόχου του υποέργου 9 του έργου Σύζευξις.

6.3.2. Περίοδος Χρήσης των Δημόσιων και Ιδιωτικών Κλειδιών

Η Λειτουργική Περίοδος ενός Πιστοποιητικού ολοκληρώνεται με τη λήξη ή την ανάκλησή του. Η Λειτουργική Περίοδος για τα ζεύγη κλειδιών είναι ίδια με τη Λειτουργική Περίοδο των αντίστοιχων Πιστοποιητικών. Τα ιδιωτικά κλειδιά βέβαια μπορούν να συνεχίσουν να χρησιμοποιούνται για αποκρυπτογράφηση και τα δημόσια κλειδιά για επαλήθευση υπογραφής. Οι μέγιστες Λειτουργικές Περίοδοι των Πιστοποιητικών των ΑΠ για Πιστοποιητικά που εκδίδονται από την έναρξη ισχύος του παρόντος ΚΠ και μετά παρατίθενται στον ακόλουθο Πίνακα 6.

Επιπροσθέτως, η ΑΠΕΔ και οι ΥπΑΠ παύουν να εκδίδουν νέα Πιστοποιητικά εγκαίρως πριν από τη λήξη του Πιστοποιητικού τους, έτσι ώστε να διασφαλίζεται ότι κανένα Πιστοποιητικό το οποίο θα εκδοθεί από την ΑΠΕΔ ή τις ΥπΑΠ δεν θα λήγει μετά τη λήξη του δικού τους Πιστοποιητικού.

Πιστοποιητικό που Εκδόθηκε Από:	
Πρωτεύουσας Αρχής Πιστοποίησης (ΑΠΕΔ) αυτοϋπογραφόμενο	Μέχρι 10 έτη
ΑΠΕΔ προς ΥπΑΠ	Μέχρι 5 έτη
ΥπΑΠ προς Τελικό Χρήστη	1 έτος

Πίνακας 6 – Λειτουργικές Περίοδοι Πιστοποιητικών

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) παύει να χρησιμοποιεί τα ζεύγη κλειδιών ΑΠ μετά τη λήξη της περιόδου χρήσης τους.

6.4. Δεδομένα Ενεργοποίησης

6.4.1. Παραγωγή και Εγκατάσταση Δεδομένων Ενεργοποίησης

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) συνιστά στους Τελικούς Χρήστες και τους Υπεύθυνους ΑΕ να χρησιμοποιούν τα συνθηματικά πρόσβασης (Personal identification number - PIN) που τους έχουν δοθεί.

6.4.2. Προστασία Δεδομένων Ενεργοποίησης

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και οι ΥπΑΠ υποχρεώνουν τους Υπεύθυνους ΑΕ και τους Τελικούς Χρήστες να αποθηκεύουν τα ιδιωτικά κλειδιά τους σε κρυπτογραφημένη μορφή και να τα προστατεύουν με τη χρήση έξυπνης κάρτας-ΑΔΔΥ και μυστικού κωδικού πρόσβασης σε αυτή (PIN).

6.4.3. Άλλα Θέματα για την Ενεργοποίηση Δεδομένων

Δεν υπάρχουν άλλα θέματα πέραν των αναφερομένων στις § 6.4.1 και 6.4.2 του ΚΠ.

6.5. Μέτρα Ασφαλείας των Υπολογιστών

Όλες οι αρμοδιότητες ΑΠ ασκούνται χρησιμοποιώντας Αξιόπιστα Συστήματα.

6.5.1. Τεχνικές Προδιαγραφές Ασφάλειας Υπολογιστών

Όλα τα συστήματα λογισμικού και αρχείων των ΑΠ αποτελούν Αξιόπιστα Συστήματα ασφαλή από μη-εξουσιοδοτημένη πρόσβαση. Οι χρήστες γενικών εφαρμογών δεν διαθέτουν λογαριασμούς σε εξυπηρετητές παραγωγής (production servers).

Επίσης υπάρχει λογικός διαχωρισμός του δικτύου παραγωγής από τα άλλα τμήματα έτσι ώστε να επιτρέπεται η πρόσβαση μόνο μέσω καθορισμένων διαδικα-

σιών. Επίσης χρησιμοποιούνται συστήματα προστασίας (firewalls) για την προστασία του δικτύου παραγωγής από εσωτερική και εξωτερική διείσδυση, καθώς και για τον περιορισμό της φύσης και της προέλευσης των δραστηριοτήτων οι οποίες θα μπορούσαν να προσπελάσουν τα συστήματα αυτά.

Τέλος απαιτείται η χρήση συνθηματικών πρόσβασης (passwords), που θα αλλάζουν σε περιοδική βάση, με συγκεκριμένο αριθμό χαρακτήρων και συνδυασμό αλφαριθμητικών και ειδικών χαρακτήρων.

6.5.2. Όρια Ασφαλείας των Υπολογιστών

Η έκδοση του βασικού λογισμικού του Κέντρου Επεξεργασίας που χρησιμοποιείται πληροί τις προδιαγραφές εγγυήσεων EAL 4 του ISO/IEC 15408-3:1999, Information technology - Security techniques - Evaluation criteria για IT security - Part 3: Security assurance requirements (Πληροφορική - Τεχνικές ασφάλειας - Κριτήρια αξιολόγησης για την ασφάλεια πληροφορικών συστημάτων - Μέρος 3: Προδιαγραφές εγγυήσεων ασφάλειας) για την αξιολόγηση του λογισμικού από ανεξάρτητο εργαστήριο βάση των Common Criteria. Οι όποιες νέες εκδόσεις του λογισμικού του Κέντρου Επεξεργασίας στο μέλλον επίσης θα αξιολογηθούν σύμφωνα με τα Common Criteria.

6.6. Τεχνικοί Έλεγχοι κατά τον Κύκλο Ζωής Πιστοποιητικού

6.6.1. Μέτρα Ελέγχου Ανάπτυξης Συστήματος

Οι εφαρμογές αναπτύσσονται και υλοποιούνται για την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) από τον ανάδοχο του υποέργου 9 του έργου «Σύζευξις» σύμφωνα με τα πρότυπα που έχει ορίσει η ΑΠΕΔ για την ανάπτυξη συστημάτων και τη διαχείριση αλλαγών.

6.6.2. Μέτρα Ελέγχου Διαχείρισης Ασφάλειας

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) διασφαλίζει την τήρηση των όρων και προϋποθέσεων του παρόντος ΚΠ από τα συστήματα της ΑΠΕΔ και των ΥπΑΠ. Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) επαληθεύει περιοδικά, την αρτιότητα των συστημάτων της ΑΠΕΔ και των ΥπΑΠ.

6.6.3. Δείκτες Ασφάλειας κατά τον Κύκλο Ζωής

Δεν προβλέπεται.

6.7. Μέτρα Ελέγχου Ασφάλειας Δικτύου

Όλες οι υπηρεσίες πιστοποίησης των ΑΠ παρέχονται χρησιμοποιώντας ασφαλή δίκτυα σύμφωνα με την ισχύουσα Πολιτική Ασφαλείας ώστε να αποτραπεί μη-εξουσιοδοτημένη πρόσβαση ή άλλη κακόβουλη ενέργεια. Επίσης προστατεύεται η κοινοποίηση εμπιστευτικών πληροφοριών με τη χρήση κρυπτογράφησης και ψηφιακών υπογραφών.

6.8. Μέτρα Μηχανικού Ελέγχου Ασφαλών Κρυπτογραφικών Μονάδων

Οι Ασφαλείς Κρυπτογραφικές Μονάδες (ΑΚΜ) που χρησιμοποιούνται από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) πληρούν τις προδιαγραφές που ορίζονται στην § 6.2.1 του ΚΠ.

6.8.1. Μέτρα Μηχανικού Ελέγχου Ασφαλών Διατάξεων Δημιουργίας Υπογραφής (ΑΔΔΥ)

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) διανέμει στους Τελικούς Χρήστες τις έξυπνες κάρτες - Ασφαλείς Διατάξεις Δημιουργίας Υπογραφής (ΑΔΔΥ) που πληρούν τις παρακάτω απαιτήσεις :

Πρώτον, επιβεβαιώνεται μέσα από κατάλληλα τεχνικά και διαδικαστικά μέσα ότι:

- Το ιδιωτικό κλειδί του πιστοποιητικού Υπογραφής που βρίσκεται στην ΑΔΔΥ μπορεί πρακτικά να εμφανιστεί μόνο μία φορά και έτσι τηρείται η μυστικότητά του.
- Δεν μπορεί, με εύλογο τρόπο, να αναζητηθεί η προέλευση αυτού του ιδιωτικού κλειδιού. Επιπλέον η υπογραφή είναι προστατευμένη από παραποίηση χρησιμοποιώντας την τρέχουσα διαθέσιμη τεχνολογία.
- Κάθε ιδιωτικό κλειδί μπορεί να προστατεύεται αξιόπιστα από τον Τελικό Χρήστη έναντι της χρήσης τρίτων.

Δεύτερον, οι ΑΔΔΥ δεν τροποποιούν - αλλοιώνουν τα στοιχεία που υπογράφονται και δεν παρουσιάζουν τροποποιημένα - αλλοιωμένα στοιχεία στον υπογράφοντα πριν από τη διαδικασία υπογραφής.

Τρίτον, οι ΑΔΔΥ που χρησιμοποιούνται από την ΑΠΕΔ και τις ΥπΑΠ βρίσκονται σε συμφωνία με τις απαιτήσεις του παραρτήματος III του ΠΔ 150/2001. Συγκεκριμένα οι ΑΔΔΥ που χρησιμοποιεί, σύμφωνα με τα παραπάνω, η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) ακολουθούν το πρότυπο CC EAL4+.

7. Προφίλ Πιστοποιητικού και Καταλόγου Ανακληθέντων Πιστοποιητικών (ΚΑΠ)

7.1. Προφίλ Πιστοποιητικού

Στην παρούσα παράγραφο ορίζονται οι προδιαγραφές του Προφίλ και του περιεχομένου των Πιστοποιητικών της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και των ΥπΑΠ που εκδίδονται σύμφωνα με τον παρόντα ΚΠ.

Τα Πιστοποιητικά της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) συμμορφώνονται με (α) το ITU-T Recommendation X.509 (1997):Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 και (β) το RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 («RFC 3280») [Προφίλ Πιστοποιητικού Υποδομής Δημοσίου Κλειδιού Διαδικτύου X.509 και ΚΑΠ].

Το περιεχόμενο των πιστοποιητικών που ακολουθούν την ΠΠ 1 συμφωνεί με το «Προφίλ Αναγνωρισμένου Πιστοποιητικού» («Qualified Certificate Profile») της τεχνικής προδιαγραφής "ETSI 101 862". Η συμμόρφωση με το «Προφίλ Αναγνωρισμένου Πιστοποιητικού» («Qualified Certificate Profile») έχει ως αποτέλεσμα τα Πιστοποιητικά που ακολουθούν την ΠΠ 1 να βρίσκονται σε συμφωνία με το RFC 3739, όπου αυτό δεν συγκρούεται με αυτό το Προφίλ. Επίσης τα βασικά πεδία των Πιστοποιητικών ΠΠ 1 βρίσκονται σε συμμόρφωση με την Ευρωπαϊκή Οδηγία 99/93/ΕΚ όπως έχει ενσωματωθεί στην ελληνική έννομη τάξη με το ΠΔ 150/2001. Αυτό σημαίνει ότι στα Πιστοποιητικά που ακολουθούν την ΠΠ 1 περιλαμβάνονται:

- Στοιχεία επαλήθευσης υπογραφής (δημόσιο κλειδί υποκειμένου-subject public key).
- Ένδειξη έναρξης και λήξης της περιόδου ισχύος (valid from-valid to).
- Ο κώδικας ταυτοποίησης του πιστοποιητικού (serial number).
- Η Προηγμένη Ηλεκτρονική Υπογραφή του παρόχου υπηρεσιών πιστοποίησης που εκδίδει το πιστοποιητικό.

Αντίστοιχες υποχρεώσεις αναλαμβάνονται και για τα Πιστοποιητικά που ακολουθούν την ΠΠ 2, αν και δεν ακολουθείται το ανωτέρω πρότυπο.

Κατ' ελάχιστο, τα Πιστοποιητικά Χ.509 της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) περιλαμβάνουν τα βασικά πεδία Χ.509 Έκδοσης 1 και τις προτεινόμενες καθορισμένες τιμές ή περιορισμούς τιμών που αναφέρονται στον ακόλουθο Πίνακα 7:

Πεδίο	Τιμή ή Περιορισμός Τιμής
Version (Έκδοση)	Βλ. ΚΠ §7.1.1.
Serial Number (Αριθμός Σειράς)	Μοναδική τιμή ανά Διακριτικό Όνομα Εκδότη (Issuer DN)
Signature Algorithm (Αλγόριθμος Υπογραφής)	Ο αλγόριθμος που χρησιμοποιήθηκε για την υπογραφή του Πιστοποιητικού (Βλ. § 7.1.3 του ΚΠ)
Issuer DN (Διακριτικό Όνομα Εκδότη)	Βλ. § 7.1.4 του ΚΠ.
Valid From (Ισχύει Από)	Βάσει του Universal Coordinate Time. Κωδικοποίηση σύμφωνα με το RFC 3280.
Valid To (Ισχύει Μέχρι)	Βάσει του Universal Coordinate Time. Κωδικοποίηση σύμφωνα με το RFC 3280. Η περίοδος ισχύος θα καθορίζεται σύμφωνα με τους περιορισμούς που ορίζει η § 6.3.2 του ΚΠ.
Subject DN (Διακριτικό Όνομα Υποκειμένου)	Βλ. § 7.1.4 του ΚΠ.
Subject Public Key (Δημόσιο Κλειδί Υποκειμένου)	Κωδικοποιημένο σύμφωνα με το RFC 3280 με τη χρήση αλγορίθμων που προσδιορίζονται στην § 7.1.3 ΚΠ και με μήκη κλειδιών που προσδιορίζονται στην § 6.1.5 ΚΠ.
Signature (Υπογραφή)	Παράγεται και κωδικοποιείται σύμφωνα με το RFC 3280

Πίνακας 7 - Βασικά Πεδία Προφίλ Πιστοποιητικού

7.1.1. Αριθμός(-οί) Έκδοσης

Τα Πιστοποιητικά ΥπΑΠ και τελικών χρηστών της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) αποτελούν Πιστοποιητικά Χ.509 Έκδοσης 3 και το πεδίο έκδοσης τους (version) θα έχει την τιμή 0x2.

7.1.2. Επεκτάσεις Πιστοποιητικών

Στα Πιστοποιητικά Χ.509 Έκδοσης 3, αναγράφονται οι επεκτάσεις που απαιτούνται σύμφωνα με τις § 7.1.2.1 - § 7.1.2.9 του ΚΠ.

7.1.2.1. Χρήση Κλειδιού (Key Usage)

1.1.1. Τα στοιχεία που υπάρχουν στην επέκταση KeyUsage (ΧρήσηΚλειδιού) για τα Πιστοποιητικά Χ.509 Έκδοσης 3 της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και των ΥπΑΠ είναι σύμφωνα με το RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL (Προφίλ Πιστοποιητικού Υποδομής Δημοσίου Κλειδιού Διαδικτύου Χ.509 και ΚΑΠ). Η επέκταση KeyUsage (ΧρήσηΚλειδιού) των Πιστοποιητικών της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και των ΥπΑΠ Χ.509 Έκδοσης 3 για τις δύο πολιτικές πιστοποιητικών τελικού χρήστη που ακολουθούνται (ΠΠ 1 και ΠΠ 2) και για τα πιστοποιητικά ΥπΑΠ παρατίθεται στον παρακάτω Πίνακα 8 με την ακόλουθη εξαίρεση:

- Το πεδίο κρισιμότητας (criticality) της επέκτασης KeyUsage (ΧρήσηΚλειδιού) ορίζεται ως ΑΛΗΘΕΣ για τα πιστοποιητικά ΑΠ και ως ΨΕΥΔΕΣ (FALSE) για τα πιστοποιητικά τελικών χρηστών.

Η μόνη διάκριση που υπάρχει μεταξύ των δύο πολιτικών (ΠΠ 1 και ΠΠ 2) για τα πιστοποιητικά τελικών χρηστών είναι πως: α) για την ΠΠ 1 ως χρήση κλειδιού ορίζεται η ψηφιακή υπογραφή (digitalSignature, 0) ενώ β) για την ΠΠ 2 η κρυπτογράφηση κλειδιού (keyEncipherment, 2) και δεδομένων (dataEncipherment, 3).

		Αρχές Πιστοποίησης	Πιστοποιητικό Υπογραφής Τελικών Χρηστών (ΠΠ 1)	Πιστοποιητικό Κρυπτογράφησης Τελικών Χρηστών (ΠΠ 2)
	Κρισιμότητα	ΨΕΥΔΗΣ (FALSE)	ΨΕΥΔΗΣ (FALSE)	ΨΕΥΔΗΣ (FALSE)
0	DigitalSignature (ηλεκτρονική Υπογραφή)	Ελεύθερο	Ορίζεται (Set)	Ελεύθερο
1	NonRepudiation (μη Αποκήρυξη)	Ελεύθερο	Ορίζεται (Set)	Ελεύθερο
2	keyEncipherment (κρυπτογράφηση Κλειδιού)	Ελεύθερο	Ελεύθερο	Ορίζεται (Set)
3	dataEncipherment (κρυπτογράφηση Δεδομένων)	Ελεύθερο	Ελεύθερο	Ορίζεται (Set)
4	keyAgreement (συμφωνία Κλειδιού)	Ελεύθερο	Ελεύθερο	Ελεύθερο
5	keyCertSign (Κλειδί Υπογραφής Πιστοποιητικού)	Ορίζεται (Set)	Ελεύθερο	Ελεύθερο
6	CRLSign (υπογραφή ΚΑΠ)	Ορίζεται (Set)	Ελεύθερο	Ελεύθερο
7	encipherOnly (Μόνο κρυπτογράφηση)	Ελεύθερο	Ελεύθερο	Ελεύθερο
8	decipherOnly (Μόνο αποκρυπτογράφηση)	Ελεύθερο	Ελεύθερο	Ελεύθερο

Πίνακας 8 - Ρυθμίσεις για την Επέκταση ΧρήσηΚλειδιού (KeyUsage)

7.1.2.2. Επέκταση Πολιτικών Πιστοποιητικού (Certificate Policies extension)

1.1.3. Τα Πιστοποιητικά Τελικού Χρήστη Χ.509 Έκδοσης 3 δύναται να χρησιμοποιήσουν επέκταση CertificatePolicies (Πολιτικές Πιστοποιητικού) όπου θα αναγράφεται ο ισχύων προσδιοριστής αντικειμένου (object identifier) σύμφωνα με την § 7.1.6 του ΚΠ και οι περιγραφείς πολιτικής (policy qualifiers) που παρατίθενται στην § 7.1.8 του ΚΠ. Το πεδίο κρισιμότητας της επέκτασης αυτής ορίζεται ως ΨΕΥΔΕΣ (FALSE).

7.1.2.3. Εναλλακτικά Ονόματα Υποκειμένου (Subject Alternative Names)

1.1.4. Η επέκταση subjectAltName υποστηρίζεται για τα πιστοποιητικά X.509 Έκδοσης 3 σύμφωνα με το RFC 3280. Το πεδίο κρισιμότητας της επέκτασης αυτής ορίζεται ως ΨΕΥΔΕΣ (FALSE).

7.1.2.4. Βασικοί Περιορισμοί (Basic Constraints)

1.1.5. Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) αναγράφει στα Πιστοποιητικά ΥπΑΠ X.509 Έκδοσης 3 την επέκταση BasicConstraints (Βασικοί Περιορισμοί) όπου το πεδίο CA (ΑΠ) έχει οριστεί ως ΑΛΗΘΕΣ (TRUE). Στα Πιστοποιητικά Τελικού Χρήστη που εκδίδουν οι ΥπΑΠ το πεδίο της επέκτασης BasicConstraints (Βασικοί Περιορισμοί) παραμένει κενό υποδηλώνοντας πως έχει οριστεί ως End Entity (Τελικό Πρόσωπο). Το πεδίο κρισιμότητας (criticality) της επέκτασης BasicConstraints (Βασικοί Περιορισμοί) ορίζεται ως ΑΛΗΘΕΣ (TRUE) για τα Πιστοποιητικά ΥπΑΠ και ΨΕΥΔΕΣ (FALSE) για τα Πιστοποιητικά των τελικών χρηστών.

1.1.6. Τα Πιστοποιητικά ΥπΑΠ X.509 Έκδοσης 3 της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) εκδίδονται ορίζοντας στο πεδίο pathLenConstraint (περιορισμός Μήκους Διαδρομής) της επέκτασης BasicConstraints (Βασικοί Περιορισμοί) το μέγιστο αριθμό πιστοποιητικών ΥπΑΠ που μπορούν να ακολουθήσουν το Πιστοποιητικό αυτό σε μια διαδρομή πιστοποίησης. Τα Πιστοποιητικά ΥπΑΠ που εκδίδονται από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ), έχουν στο πεδίο pathLenConstraint (περιορισμός Μήκους Διαδρομής) την τιμή «0» υποδεικνύοντας ότι μόνο ένα Πιστοποιητικό Τελικού Χρήστη μπορεί να ακολουθήσει τη διαδρομή πιστοποίησης.

7.1.2.5. Εκτεταμένη Χρήση Κλειδιού (Extended Key Usage)

Η επέκταση ExtendedKeyUsage (Εκτεταμένη Χρήση Κλειδιού) χρησιμοποιείται από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και τις ΥπΑΠ για τα πιστοποιητικά Τελικών Χρηστών που εκδίδει (X.509 Έκδοσης 3) στις ακόλουθες περιπτώσεις (Πίνακας 9).

		Πιστοποιητικό Υπογραφής Τελικού Χρήστη (ΠΠ 1)	Πιστοποιητικό Κρυπτογράφησης Τελικού Χρήστη (ΠΠ 2)
Criticality (Κρισιμότητα)		ΨΕΥΔΗΣ (FALSE)	ΨΕΥΔΗΣ (FALSE)
0	ServerAuth (Ταυτοποίηση Εξυπηρετητή)	Ελεύθερο	Ελεύθερο
1	ClientAuth (Ταυτοποίηση Χρήστη)	Ορίζεται	Ελεύθερο
2	CodeSigning (Υπογραφή Κωδικού)	Ελεύθερο	Ελεύθερο
3	EmailProtection (Προστασία Email)	Ορίζεται	Ελεύθερο
4	ipsecEndSystem (τελικό Σύστημα IPsec)	Ελεύθερο	Ελεύθερο
5	ipsecTunnel (δίαυλος IPsec)	Ελεύθερο	Ελεύθερο
6	ipsecUser (Χρήστης IPsec)	Ελεύθερο	Ελεύθερο
7	TimeStamping (Χρονοσήμανση)	Ελεύθερο	Ελεύθερο
8	OCSP Signing (Υπογραφή OCSP)	Ελεύθερο	Ελεύθερο

Πίνακας 9 - Ρυθμίσεις για την Επέκταση - Εκτεταμένη Χρήση Κλειδιού (ExtendedKeyUsage)

7.1.2.6. Σημεία Διανομής ΚΑΠ (CRL Distribution Points)

Στα Πιστοποιητικά Τελικού Χρήστη περιλαμβάνεται η επέκταση CRLDistributionPoints (Σημεία Διανομής ΚΑΠ) η οποία παραπέμπει στο δικτυακό κόμβο (URL) από όπου κάποιος Τρίτος Συμμετέχων μπορεί να λάβει έναν ΚΑΠ ώστε να ελέγξει την κατάσταση ενός Πιστοποιητικού. Το πεδίο κρισιμότητας στην επέκταση αυτή ορίζεται ως ΨΕΥΔΕΣ (FALSE). Αντίστοιχη επέκταση περιλαμβάνεται και στα πιστοποιητικά των υποκείμενων ΑΠ.

7.1.2.7. Προσδιοριστής Κλειδιού Αρχής (Authority Key Identifier)

Η δυνατότητα χρήσης της επέκτασης Authority Key Identifier (Προσδιοριστής Κλειδιού Αρχής) παρέχεται για τα Πιστοποιητικά των ΥπΑΠ και των Τελικών Χρηστών. Η μέθοδος δημιουργίας του keyIdentifier (Προσδιοριστής Κλειδιού) υπολογίζεται σύμφωνα με τις μεθόδους που περιγράφονται στο RFC 3280. Το πεδίο κρισιμότητας στην επέκταση αυτή ορίζεται ως ΨΕΥΔΕΣ (FALSE).

7.1.2.8. Προσδιοριστής Κλειδιού Υποκειμένου (Subject Key Identifier)

Η δυνατότητα χρήσης της επέκτασης Subject Key Identifier (Προσδιοριστής Κλειδιού Υποκειμένου) παρέχεται για το αυτουπογραφόμενο Πιστοποιητικό της ΑΠΕΔ, τα Πιστοποιητικά ΥπΑΠ και τα πιστοποιητικά Τελικών Χρηστών. Η μέθοδος δημιουργίας του keyIdentifier (Προσδιοριστής Κλειδιού) υπολογίζεται σύμφωνα με τις μεθόδους που περιγράφονται στο RFC 3280. Το πεδίο κρισιμότητας στην επέκταση αυτή ορίζεται ως ΨΕΥΔΕΣ (FALSE).

7.1.2.9. Ιδιωτικές Επεκτάσεις Πιστοποιητικού

Τα Πιστοποιητικά υπογραφής που ακολουθούν την ΠΠ 1 περιέχουν μια ιδιωτική επέκταση (private extension) η οποία περιέχει ένα Προσδιοριστή Αντικειμένου (OID) που δηλώνει ότι το πιστοποιητικό εκδίδεται σύμφωνα με την Ευρωπαϊκή Οδηγία 99/93/ΕΚ που έχει ενσωματωθεί στην Ελληνική νομοθεσία με το ΠΔ 150/2001. Αυτή η επέκταση βρίσκεται σε συμφωνία με τον ορισμό της παραγράφου 4.2.1 (2) του «Προφίλ Αναγνωρισμένου Πιστοποιητικού» («Qualified Certificate Profile») της τεχνικής προδιαγραφής "ETSI 101 862" και του κειμένου πολιτικής "ETSI 101 456" και μπορεί να χαρακτηριστεί ως κρίσιμη ή μη κρίσιμη.

Επίσης είναι στην επιλογή της ΑΠΕΔ να χρησιμοποιηθούν οι ακόλουθες πρόσθετες ιδιωτικές επεκτάσεις:

- Επέκταση που περιλαμβάνει δήλωση για τυχόν ύπαρξη ορίου στην αξία των συναλλαγών όπου το πιστοποιητικό μπορεί να χρησιμοποιηθεί σύμφωνα με την παράγραφο 4.2.2 του «Προφίλ Αναγνωρισμένου Πιστοποιητικού» («Qualified Certificate Profile») της τεχνικής προδιαγραφής "ETSI 101 862".
- Επέκταση που περιλαμβάνει δήλωση για την περίοδο διατήρησης αρχείων σύμφωνα με την §4.6.2 του ΚΠ και την παράγραφο 4.2.3 του «Προφίλ Αναγνωρισμένου

Πιστοποιητικού» («Qualified Certificate Profile») της τεχνικής προδιαγραφής "ETSI 101 862".

7.1.3. Προσδιοριστές Αντικειμένου Αλγορίθμου Υπογραφής (Algorithm Object Identifiers)

Τα Πιστοποιητικά X.509 της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και των ΥπΑΠ υπογράφονται με sha1RSA (OID: 1.2.840.113549.1.1.5) σύμφωνα με το RFC 3279.

7.1.4. Μορφές Ονομάτων

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και οι ΥπΑΠ αναγράφουν στα πιστοποιητικά τους το Διακριτικό Όνομα του Εκδότη και του Υποκειμένου σύμφωνα με την § 3.1.1 του ΚΠ.

7.1.5. Περιορισμοί Ονομάτων

Δεν προβλέπονται.

7.1.6. Προσδιοριστής Αντικειμένου Πολιτικής Πιστοποιητικού (Certificate Policy Object Identifier)

Τα Πιστοποιητικά των τελικών χρηστών θα περιλαμβάνουν προσδιοριστή αντικειμένου για την Πολιτική Πιστοποιητικού (Certificate Policy Object Identifier) που θα ακολουθούν, σύμφωνα με την § 1.2. του ΚΠ. Τα Πιστοποιητικά ΥπΑΠ της ΑΠΕΔ θα περιλαμβάνουν προσδιοριστή αντικειμένου για την Πολιτική Πιστοποιητικού (Certificate Policy Object Identifier) που θα διέπει την κάθε ΥπΑΠ.

7.1.7. Επέκταση Περιορισμών Χρήσης Πολιτικής

Δεν προβλέπεται.

7.1.8. Σύνταξη και Σημασιολογία Περιγραφέων Πολιτικής (Policy Qualifiers Syntax and Semantics)

Τα Πιστοποιητικά X.509 Έκδοσης 3 της ΑΠΕΔ θα περιλαμβάνουν, στην επέκταση πολιτικής πιστοποιητικού, ένα περιγραφέα πολιτικής που θα παραπέμπει στον ΚΠ της ΑΠΕΔ. Βλ. και § 7.1.6 του ΚΠ.

7.1.9. Επεξεργασία Σημασιολογίας για την Κρίσιμη Επέκταση Πολιτικής Πιστοποιητικού

Δεν προβλέπεται.

7.2. Προφίλ Καταλόγου Ανακληθέντων Πιστοποιητικών (ΚΑΠ)

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και οι ΥπΑΠ εκδίδουν ΚΑΠ οι οποίοι είναι σύμφωνοι με το RFC 3280. Κατ' ελάχιστο, οι εν λόγω ΚΑΠ περιλαμβάνουν τα βασικά πεδία και περιεχόμενα που προσδιορίζονται στον ακόλουθο Πίνακα 10:

Πεδίο	Τιμή ή Περιορισμός Τιμής
Version (Εκδοση)	Βλ. §7.2.1 του ΚΠ.
Signature Algorithm (Αλγόριθμος Υπογραφής)	Αλγόριθμος που χρησιμοποιείται για την υπογραφή του ΚΑΠ. Οι ΚΑΠ της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και των ΥπΑΠ υπογράφονται με τη χρήση sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) ή md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) σύμφωνα με το RFC 3279.
Issuer (Εκδότης)	Ο Φορέας που υπογράφει και εκδίδει τον ΚΑΠ. Το Όνομα Εκδότη ΚΑΠ είναι σύμφωνο με τις προδιαγραφές του Διακριτικού Ονόματος Εκδότη που ορίζονται στην § 7.1.4 του ΚΠ.
Effective Date (Ημερομηνία Ισχύος)	Ημερομηνία έκδοσης του ΚΑΠ. Οι ΚΑΠ της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και των ΥπΑΠ ισχύουν με την έκδοσή τους.
Next Update (Επόμενη Ενημέρωση)	Ημερομηνία κατά την οποία θα εκδοθεί ο επόμενος ΚΑΠ. Η συχνότητα έκδοσης ΚΑΠ είναι σύμφωνη με τις προδιαγραφές της § 4.4.8 του ΚΠ.
Revoked Certificates (Ανακληθέντα Πιστοποιητικά)	Καταγραφή των ανακληθέντων πιστοποιητικών, περιλαμβανομένων του Αριθμού Σειράς του ανακληθέντος Πιστοποιητικού και της Ημερομηνίας Ανάκλησης.

Πίνακας 10 - Βασικά Πεδία Προφίλ ΚΑΠ

7.2.1. Αριθμός(-οί) Έκδοσης

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) και οι ΥπΑΠ εκδίδουν ΚΑΠ X.509 Έκδοσης 1.

7.2.2. Επεκτάσεις ΚΑΠ και Καταχωρήσεων ΚΑΠ

Δεν προβλέπονται.

8. Διαχείριση των Προσδιορισμών

8.1. Διαδικασίες Τροποποίησης των Προσδιορισμών

Τροποποιήσεις του παρόντος ΚΠ επιτρέπονται ύστερα από πρόταση της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ). Οι τροποποιήσεις θα είναι είτε υπό μορφή εγγράφου που περιέχει την τροποποιημένη μορφή του ΚΠ ή με ενημερωμένη έκδοση. Οι τροποποιημένες εκδόσεις ή ενημερώσεις παρατίθενται στο τμήμα του Χώρου Αποθήκευσης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) για Ενημερώσεις και Ανακοινώσεις επί των Κανονισμών στη διεύθυνση: http://www.syzefxis.gov.gr. Οι ενημερωμένες εκδόσεις του ΚΠ υπερισχύουν έναντι οποιωνδήποτε προηγούμενων.

8.1.1. Στοιχεία που Μπορούν να Τροποποιηθούν Χωρίς Προειδοποίηση

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δύναται να προτείνει τροποποιήσεις του παρόντος ΚΠ χωρίς προειδοποίηση των Τελικών Χρηστών και Τρίτων Συμμετεχόντων, για μεταβολές που δεν είναι ουσιώδους σημασίας, περιλαμβανομένων ενδεικτικά, διορθώσεων τυπογραφικών λαθών, αλλαγών των δικτυακών κόμβων (URL) και μεταβολών των στοιχείων επικοινωνίας.

8.1.2. Στοιχεία που Μπορούν να Τροποποιηθούν Με Προειδοποίηση

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δύναται να προτείνει ουσιώδεις τροποποιήσεις του ΚΠ ύστερα από προειδοποίηση των Τελικών Χρηστών τουλάχιστον με σχετική ανακοίνωση στον Χώρο Αποθήκευσης της που προορίζεται για Ενημερώσεις και Ανακοινώσεις επί των Κανονισμών στη διεύθυνση: http://www.syzefxis.gov.gr.

8.1.2.1. Ανακοίνωση

Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) ανακοινώνει τις τροποποιήσεις του ΚΠ στο τμήμα του Χώρου Αποθήκευσης της που προορίζεται για Ενημερώσεις και Ανακοινώσεις επί των Κανονισμών, στη διεύθυνση: http://www.syzefxis.gov.gr.

8.2. Πολιτική Δημοσίευσης και Κοινοποίησης

8.2.1. Στοιχεία που δεν δημοσιεύονται στον ΚΠ

Τα έγγραφα ασφαλείας που θεωρούνται εμπιστευτικά από την Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) δεν αποκαλύπτονται σε τρίτους.

8.2.2. Δημοσίευση του ΚΠ

Ο παρών ΚΠ δημοσιεύεται σε ηλεκτρονική μορφή στο Χώρο Αποθήκευσης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) στη διεύθυνση http://www.syzefxis.gov.gr όπου βρίσκεται διαθέσιμος σε μορφή εγγράφου Adobe Acrobat® pdf ή/και Microsoft Word® ή HTML. Η Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) επίσης διαθέτει τον ΚΠ σε μορφή Adobe Acrobat® pdf ή Microsoft Word® στη διεύθυνση support@syzefxis.gov.gr.

ΠΑΡΑΡΤΗΜΑ
Ακρωνύμια και Ορισμοί
Πίνακας Ακρωνυμίων

Ακρωνύμιο		Όρος
(Ελληνικά)	(Αγγλικά)	(στα Ελληνικά και στα Αγγλικά)
	CC	Common Criteria
	EAL	Evaluation Assurance Level. (Επίπεδο Αξιολόγησης Εγγυήσεων, σύμφωνα με τα Common Criteria)
	FIPS	United States Federal Information Processing Standards (Ομοσπονδιακά Πρότυπα Επεξεργασίας Πληροφοριών των Ηνωμένων Πολιτειών)
	PIN	Personal Identification Number (Προσωπικός Αριθμός Αναγνώρισης)
	PKCS	Public-Key Cryptography Standard (Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού)
	PUK	Personal Unblocking Key (Προσωπικό Κλειδί που χρησιμοποιείται για απεμπλοκή της έξυπνης κάρτας μετά από συνεχής εσφαλμένη εισαγωγή του PIN)
	RFC	Request For Comment (Αίτημα για σχολιασμό)
	S/MIME	Secure Multipurpose Internet Mail Extensions (Πρότυπο ασφαλούς ηλεκτρονικού ταχυδρομείου γενικής χρήσης μέσω διαδικτύου)
ΑΕ	RA	Αρχή Εγγραφής (Registration Authority)
ΑΠ	CA	Αρχή Πιστοποίησης (Certification Authority)
ΑΤΛΑ	LSVA	Αξιολόγηση Τρωτότητας της Λογικής Ασφάλειας (Logical Security Vulnerability Assessment)
ΚΑΠ	CRL	Κατάλογος Ανακληθέντων Πιστοποιητικών (Certificate Revocation List)
ΚΠ	CPS	Κανονισμός Πιστοποίησης (Certification Practice Statement)
ΟΤΠ		Όροι Τρίτου Συμμετέχοντα
ΟΧΠ		Όροι Χορήγησης Πιστοποιητικού
ΠΑ	OID	Προσδιοριστής Αντικειμένου (Object Identifier)
ΠΑΠ	PCA	Πρωτεύουσα Αρχή Πιστοποίησης (Primary Certification Authority)
ΠΥΠ		Πάροχος Υπηρεσιών Πιστοποίησης
ΠΠ	CP	Πολιτική Πιστοποιητικού (Certificate Policy)
ΥΔΚ	PKI	Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure)

Ορισμοί

Όρος	Ορισμός
PKCS # 10	Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού (Public-Key Cryptography Standard) #10, που έχει αναπτυχθεί από τη RSA Security Inc., το οποίο καθορίζει τη δομή του ηλεκτρονικού αιτήματος υπογραφής πιστοποιητικού.
PKCS # 12	Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού (Public-Key Cryptography Standard) #12, που έχει αναπτυχθεί από τη RSA Security Inc., το οποίο καθορίζει το ασφαλές μέσο για τη μεταβίβαση των ιδιωτικών κλειδιών.
RSA	Το κρυπτογραφικό σύστημα δημοσίου κλειδιού που επινοήθηκε από τους Rivest, Shamir και Adelman.
Αλυσίδα Πιστοποιητικού (Certificate Chain)	Ο κατάλογος κατά σειρά κατάταξης των Πιστοποιητικών, που περιλαμβάνει ένα Πιστοποιητικό Τελικού Χρήστη, Πιστοποιητικά ΑΠ και καταλήγει σε ένα Πιστοποιητικό ΠΑΠ (Root).
Αναγνωρισμένο Πιστοποιητικό	Πιστοποιητικό που πληροί τους όρους του Παραρτήματος Ι του ΠΔ 150/2001 και εκδίδεται από πάροχο υπηρεσιών πιστοποίησης ο οποίος πληροί τους όρους του παραρτήματος ΙΙ του ΠΔ 150/2001.
Αξιόπιστο Σύστημα	Εξοπλισμός, λογισμικό και διαδικασίες ηλεκτρονικού υπολογιστή που είναι λογικά ασφαλείς έναντι διείσδυσης και κακής χρήσης. Εξασφαλίζει ένα λογικό επίπεδο διαθεσιμότητας, αξιοπιστίας και ορθής λειτουργίας, είναι κατάλληλο για την εκτέλεση των οριζόμενων εργασιών και επιβάλλει την ισχύουσα πολιτική ασφάλειας. Ένα αξιόπιστο σύστημα δεν αποτελεί απαραίτητα «έμπιστο σύστημα».

Αρχή Εγγραφής (ΑΕ)	Ο φορέας ή υπηρεσία που έχει εγκριθεί από μια ΑΠ και υποβοηθά τους ενδιαφερόμενους για Πιστοποιητικά κατά την υποβολή του «Εντύπου ΥΔΚ», εγκρίνει ή απορρίπτει τις Ηλεκτρονικές Εγγραφές για πιστοποιητικά καθώς επίσης αιτείται στην Αρχή Πιστοποίησης την ανάκληση, ανανέωση ή ανάκτηση Πιστοποιητικών.
Αρχή Πιστοποίησης (ΑΠ)	Ο Φορέας που έχει πιστοποιηθεί να εκδίδει, να χειρίζεται, να ανακαλεί και να ανανεώνει Πιστοποιητικά βάσει των διατάξεων του παρόντος και του άρθρου 20 του Ν.3448/2996 (ΦΕΚ 57 Α΄).
Ασφαλής Διάταξη Δημιουργίας Υπογραφής (ΑΔΔΥ - SSCD)	Διάταξη δημιουργίας υπογραφής που πληροί τους όρους του παραρτήματος ΙΙΙ του ΠΔ 150/2001.
Ασφαλής Κρυπτογραφική Μονάδα (ΑΚΜ)	Το χρησιμοποιούμενο από τους Παρόχους Υπηρεσιών Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών, Προϊόν Ηλεκτρονικής Υπογραφής που προστατεύεται έναντι τροποποίησης και διασφαλίζει τεχνική και κρυπτογραφική ασφάλεια σύμφωνα με το Παράρτημα ΙΙ του ΠΔ 150/2001 και πληροί τις απαιτήσεις της παραγράφου 2του άρθρου 3 της υπ' αριθ. 295/64/2003 Απόφασης της ΕΕΤΤ «Κανονισμός για τον Έλεγχο Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων».
Υπεύθυνος ΑΕ	Ένα Έμπιστο Πρόσωπο το οποίο έχει πρόσβαση στο Κέντρο Ελέγχου της ΑΕ και διενεργεί διαδικασίες του κύκλου ζωής ενός Πιστοποιητικού (π.χ. αποδοχής, ανάκλησης, ανάκτησης ενός Πιστοποιητικού) καθώς και άλλες αρμοδιότητες μιας ΑΕ.
Δικαιώματα Πνευματικής Ιδιοκτησίας	Δικαιώματα επί ενός ή περισσοτέρων από τα ακόλουθα: κάθε είδους δικαιώματος δημιουργού, εμπορικού μυστικού, εμπορικού σήματος, καθώς και κάθε άλλου δικαιώματος πνευματικής ιδιοκτησίας.
Έκθεση σε Κίνδυνο	Η παραβίαση (ή υποτιθέμενη παραβίαση) μιας πολιτικής ασφαλείας, κατά την οποία μπορεί να έχει συμβεί μη-εξουσιοδοτημένη αποκάλυψη ή απώλεια του ελέγχου επί διαβαθμισμένων πληροφοριών. Όσον αφορά τα ιδιωτικά κλειδιά, Έκθεση σε Κίνδυνο αποτελεί η απώλεια, κλοπή, αποκάλυψη, τροποποίηση, μη-εξουσιοδοτημένη χρήση ή κάθε άλλη έκθεση σε κίνδυνο της ασφάλειας του ιδιωτικού αυτού κλειδιού.
Εμπιστευτικές Πληροφορίες	Οι πληροφορίες που είναι απαραίτητο να παραμείνουν εμπιστευτικές και προσωπικές σύμφωνα με την § 2.8.1 του ΚΠ.
Έντυπο ΥΔΚ	Το συμπληρωμένο από τον ενδιαφερόμενο Τελικό Χρήστη έντυπο που υποβάλλεται σε ένα Εντεταλμένο Γραφείο με σκοπό να λάβουν χώρα ενέργειες του κύκλου ζωής πιστοποιητικού, δηλαδή έκδοσης ζεύγους Πιστοποιητικών (υπογραφής-κρυπτογράφησης), ανανέωσης, ανάκλησης ή ανάκτησης. Στο συγκεκριμένο Έντυπο περιλαμβάνονται τα δηλωθέντα στοιχεία του τελικού χρήστη και οι ΟΧΠ.

Ηλεκτρονική Εγγραφή	Η διαδικασία κατά την οποία ο Τελικός Χρήστης υποβάλλει ηλεκτρονικά τα στοιχεία του με σκοπό να λάβει ένα ζεύγος πιστοποιητικών (για Ψηφιακή Υπογραφή και Κρυπτογράφηση).
Ηλεκτρονική Υπογραφή	Δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή σχετίζονται λογικά με αυτά και τα οποία χρησιμεύουν ως μέθοδος απόδειξης της γνησιότητας.
Κανονισμός Πιστοποίησης (ΚΠ)	Πράξη της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) σύμφωνα με τις διατάξεις των παραγράφων 1 και 2 του άρθρου 20 του Ν. 3448/2006 (ΦΕΚ 57 Α΄) με τον οποίο καθορίζονται οι όροι και οι προϋποθέσεις για την παροχή των υπηρεσιών πιστοποίησης από την ΑΠΕΔ ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ) και τις Υποκείμενες Αρχές Πιστοποίησης (ΥπΑΠ), οι οποίες καθορίζονται σύμφωνα με τις διατάξεις της παραγράφου 4 του άρθρου 20 του παραπάνω Νόμου στο οποίο περιγράφεται αναλυτικά η πρακτική που ακολουθείται για την έκδοση πιστοποιητικών ηλεκτρονικής υπογραφής ή/και την παροχή άλλων υπηρεσιών πιστοποίησης σύμφωνα με τα αναφερόμενα στο Παράρτημα Ι της απόφασης 248/71 της ΕΕΤΤ.
Κατάλογος Ανακληθέντων Πιστοποιητικών (ΚΑΠ)	Ο περιοδικός (ή έκτακτος) κατάλογος, που εκδίδεται ηλεκτρονικά και είναι υπογεγραμμένος από μια ΑΠ, των Πιστοποιητικών που έχουν ανακληθεί πριν από την ημερομηνία λήξης τους. Ο ΚΑΠ αναφέρει το όνομα του εκδότη της ΚΑΠ, την ημερομηνία έκδοσης, την ημερομηνία της επόμενης προγραμματισμένης έκδοσης ΚΑΠ, τους αριθμούς σειράς των ανακληθέντων Πιστοποιητικών, καθώς και τους συγκεκριμένους χρόνους και λόγους ανάκλησής τους.
Κέντρο Επεξεργασίας	Μια ασφαλής λογική και φυσική υποδομή στην οποία φυλάσσονται Ασφαλείς Κρυπτογραφικές Μονάδες (ΑΚΜ) και μέσω της οποίας διενεργείται το σύνολο των υπηρεσιών διαχείρισης του κύκλου ζωής πιστοποιητικών (έκδοσης, ανάκλησης, ανάκτησης και ανανέωσης).
Λειτουργική Περίοδος	Το χρονικό διάστημα το οποίο ξεκινά από την ημερομηνία και το χρόνο έκδοσης ενός Πιστοποιητικού και λήγει την ημερομηνία και το χρόνο λήξης ή πρόωρης ανάκλησης του Πιστοποιητικού.
Πάροχος Υπηρεσιών Πιστοποίησης	Φυσικό ή νομικό πρόσωπο που εκδίδει πιστοποιητικά ή παρέχει υπηρεσίες συναφείς με τις ηλεκτρονικές υπογραφές.
Πιστοποιητικό	Ηλεκτρονική βεβαίωση η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο και επιβεβαιώνει την ταυτότητά του.
Πιστοποιητικό Υπευθύνου	Το Πιστοποιητικό που εκδίδεται προς έναν Υπεύθυνο ΑΕ και το οποίο μπορεί να χρησιμοποιηθεί αποκλειστικά για την τέλεση αρμοδιοτήτων ΑΕ.

Προϊόν Ηλεκτρονικής Υπογραφής	Υλικό ή λογισμικό ή συναφή συστατικά στοιχεία τους, που προορίζονται προς χρήση από τον πάροχο υπηρεσιών πιστοποίησης για την προσφορά υπηρεσιών ηλεκτρονικής υπογραφής ή προορίζονται να χρησιμοποιηθούν για τη δημιουργία ή επαλήθευση ηλεκτρονικών υπογραφών.
Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ)	Μια ΑΠ η οποία ενεργεί ως Πρωτεύουσα ΑΠ (Root CA) και εκδίδει Πιστοποιητικά προς υποκείμενες ΑΠ. Στην παρούσα υποδομή η ΑΠΕΔ λειτουργεί ως Πρωτεύουσα Αρχή Πιστοποίησης.
ΟΤΣ	Οι όροι και οι προϋποθέσεις βάση των οποίων ένα φυσικό πρόσωπο ενεργεί ως Τρίτος Συμμετέχων.
ΟΧΠ	Οι όροι και οι προϋποθέσεις χορήγησης πιστοποιητικών βάσει των οποίων ένα φυσικό πρόσωπο ενεργεί ως Τελικός Χρήστης.
Τελικός Χρήστης	Το πρόσωπο που αποτελεί το Υποκείμενο και στο οποίο έχει εκδοθεί ένα Πιστοποιητικό ύστερα από αίτηση του. Ο Τελικός Χρήστης είναι εξουσιοδοτημένος να χρησιμοποιεί το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο Πιστοποιητικό.
Τρίτος Συμμετέχων	Το φυσικό πρόσωπο ή φορέας που ενεργεί βασιζόμενος σε κάποιο πιστοποιητικό ή/και ηλεκτρονική υπογραφή.
Υποδομή Δημόσιου Κλειδιού (ΥΔΚ)/ Public Key Infrastructure (PKI)	Η αρχιτεκτονική, η οργανωτική δομή, οι τεχνικές, οι κανονισμοί και οι διαδικασίες που στο σύνολό τους υποστηρίζουν την εφαρμογή και λειτουργία κρυπτογραφικού συστήματος δημοσίου κλειδιού που βασίζεται σε Πιστοποιητικό.
Υποκείμενο	Ο κάτοχος ενός ιδιωτικού κλειδιού που αντιστοιχεί σε ένα δημόσιο κλειδί. Το ταυτοποιημένο όνομα ενός Υποκειμένου Πιστοποιητικού είναι συνδεδεμένο με το δημόσιο κλειδί που περιλαμβάνεται στο Πιστοποιητικό.
Ψηφιακή Υπογραφή ή Προηγμένη Ηλεκτρονική Υπογραφή	Ηλεκτρονική υπογραφή που πληροί τους εξής όρους : ● συνδέεται μονοσήμαντα με τον υπογράφοντα ● είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντος ● δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και ● συνδέεται με τα δεδομένα στα οποία αναφέρεται, κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων
Χώρος Αποθήκευσης της ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΕΛΛΗΝΙΚΟΥ ΔΗΜΟΣΙΟΥ (ΑΠΕΔ)	Η δικτυακά προσπελάσιμη βάση δεδομένων της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ) στην οποία περιέχονται τα στοιχεία των Πιστοποιητικών καθώς και άλλες πληροφορίες σχετικές με την Υποδομή Δημοσίου Κλειδιού της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)» .

Άρθρο 2
Έναρξη ισχύος

Η ισχύς της απόφασης αυτής αρχίζει από τη δημοσίευσή της στην Εφημερίδα της Κυβερνήσεως.

Η απόφαση αυτή να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Αθήνα, 18 Οκτωβρίου 2006

ΟΙ ΥΠΟΥΡΓΟΙ

ΕΣΩΤΕΡΙΚΩΝ, ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΑΠΟΚΕΝΤΡΩΣΗΣ
ΠΡΟΚΟΠΗΣ ΠΑΥΛΟΠΟΥΛΟΣ

ΜΕΤΑΦΟΡΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΜΙΧΑΛΗΣ ΛΙΑΠΗΣ

ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ

ΕΦΗΜΕΡΙΔΑ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ

ΠΕΡΙΦΕΡΕΙΑΚΑ ΓΡΑΦΕΙΑ ΠΩΛΗΣΗΣ Φ.Ε.Κ.

ΘΕΣΣΑΛΟΝΙΚΗ - Βασ. Όλγας 227	**(2310) 423 956**	**ΛΑΡΙΣΑ** - Διοικητήριο	**(2410) 597449**
ΠΕΙΡΑΙΑΣ - Ευριπίδου 63	**(210) 413 5228**	**ΚΕΡΚΥΡΑ** - Σαμαρά 13	**(26610) 89 122**
ΠΑΤΡΑ - Κορίνθου 327	**(2610) 638 109**		**(26610) 89 105**
	(2610) 638 110	**ΗΡΑΚΛΕΙΟ** - Πεδιάδος 2	**(2810) 300 781**
ΙΩΑΝΝΙΝΑ - Διοικητήριο	**(26510) 87215**	**ΛΕΣΒΟΣ** - Πλ.Κωνσταντινουπόλεως 1	**(22510) 46 654**
ΚΟΜΟΤΗΝΗ - Δημοκρατίας 1	**(25310) 22 858**		**(22510) 47 533**

ΤΙΜΗ ΠΩΛΗΣΗΣ ΦΥΛΛΩΝ ΕΦΗΜΕΡΙΔΟΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ

Σε έντυπη μορφή:
- Για τα ΦΕΚ από 1 μέχρι 16 σελίδες σε 1 euro, προσαυξανόμενη κατά 0,20 euro για κάθε επιπλέον οκτασέλιδο ή μέρος αυτού.
- Για τα φωτοαντίγραφα ΦΕΚ σε 0,15 euro ανά σελίδα.

Σε μορφή CD:

Τεύχος	Περίοδος	EURO	Τεύχος	Περίοδος	EURO
Α΄	Ετήσιο	150	Αναπτυξιακών Πράξεων	Ετήσιο	50
Α	3μηνιαίο	40	Ν.Π.Δ.Δ.	Ετήσιο	50
Α΄	Μηνιαίο	15	Παράρτημα	Ετήσιο	50
Β’	Ετήσιο	300	Εμπορικής και Βιομηχανικής Ιδιοκτησίας	Ετήσιο	100
Β΄	3μηνιαίο	80	Ανωτάτου Ειδικού Δικαστηρίου	Ετήσιο	5
Β΄	Μηνιαίο	30	Διακηρύξεων Δημοσίων Συμβάσεων	Ετήσιο	200
Γ΄	Ετήσιο	50	Διακηρύξεων Δημοσίων Συμβάσεων	Εβδομαδιαίο	5
Δ΄	Ετήσιο	220	Α.Ε. & Ε.Π.Ε	Μηνιαίο	100
Δ΄	3μηνιαίο	60			

- Η τιμή πώλησης μεμονωμένων Φ.Ε.Κ σε μορφή cd-rom από εκείνα που διατίθενται σε ηλεκτρονική μορφή και μέχρι 100 σελίδες σε 5 euro προσαυξανόμενη κατά 1 euro ανά 50 σελίδες.
- Η τιμή πώλησης σε μορφή cd-rom δημοσιευμάτων μιας εταιρείας στο τεύχος Α.Ε. και Ε.Π.Ε. σε 5 euro ανά έτος.

ΠΑΡΑΓΓΕΛΙΑ ΚΑΙ ΑΠΟΣΤΟΛΗ Φ.Ε.Κ. : τηλεφωνικά : 210 - 4071010, fax : 210 - 4071010 internet : http://www.et.gr.

ΕΤΗΣΙΕΣ ΣΥΝΔΡΟΜΕΣ Φ.Ε.Κ.

	Σε έντυπη μορφή	Από το Internet
Α΄ (Νόμοι, Π.Δ., Συμβάσεις κτλ.)	225 €	190 €
Β΄ (Υπουργικές αποφάσεις κτλ.)	320 €	225 €
Γ΄ (Διορισμοί, απολύσεις κτλ. Δημ. Υπαλλήλων)	65 €	ΔΩΡΕΑΝ
Δ΄ (Απαλλοτριώσεις, πολεοδομία κτλ.)	320 €	160 €
Αναπτυξιακών Πράξεων και Συμβάσεων (Τ.Α.Π.Σ.)	160 €	95 €
Ν.Π.Δ.Δ. (Διορισμοί κτλ. προσωπικού Ν.Π.Δ.Δ.)	65 €	ΔΩΡΕΑΝ
Παράρτημα (Προκηρύξεις θέσεων ΔΕΠ κτλ.)	33 €	ΔΩΡΕΑΝ
Δελτίο Εμπορικής και Βιομ/κής Ιδιοκτησίας (Δ.Ε.Β.Ι.)	65 €	33 €
Ανωτάτου Ειδικού Δικαστηρίου (Α.Ε.Δ.)	10 €	ΔΩΡΕΑΝ
Ανωνύμων Εταιρειών & Ε.Π.Ε.	2.250 €	645 €
Διακηρύξεων Δημοσίων Συμβάσεων (Δ.Δ.Σ.)	225 €	95 €
Πρώτο (Α΄), Δεύτερο (Β΄) και Τέταρτο (Δ΄)	–	450 €

- Το τεύχος του ΑΣΕΠ (έντυπη μορφή) θα αποστέλλεται σε συνδρομητές με την επιβάρυνση των 70 euro, ποσό το οποίο αφορά ταχυδρομικά έξοδα.
- Για την παροχή δικαιώματος ηλεκτρονικής πρόσβασης σε Φ.Ε.Κ. προηγουμένων ετών και συγκεκριμένα στα τεύχη Α΄, Β΄, Δ΄, Αναπτυξιακών Πράξεων & Συμβάσεων, Δελτίο Εμπορικής και Βιομηχανικής Ιδιοκτησίας Διακηρύξεων, Δημοσίων Συμβάσεων και Α.Ε. & Ε.Π.Ε., η τιμή προσαυξάνεται πέραν του ποσού της ετήσιας συνδρομής έτους 2006, κατά 40 euro ανά έτος παλαιότητας και ανά τεύχος.

* Οι συνδρομές του εσωτερικού προπληρώνονται στις ΔΟΥ (το ποσό συνδρομής καταβάλλεται στον κωδικό αριθμό εσόδων ΚΑΕ 2531 και το ποσό υπέρ ΤΑΠΕΤ (5% του ποσού της συνδρομής) στον κωδικό αριθμό εσόδων ΚΑΕ 3512).Το πρωτότυπο αποδεικτικό είσπραξης (διπλότυπο) θα πρέπει να αποστέλλεται ή να κατατίθεται στην αρμόδια Υπηρεσία του Εθνικού Τυπογραφείου.
* Η πληρωμή του υπέρ ΤΑΠΕΤ ποσοστού που αντιστοιχεί σε συνδρομές, εισπράττεται και από τις ΔΟΥ.
* Οι συνδρομητές του εξωτερικού έχουν τη δυνατότητα λήψης των δημοσιευμάτων μέσω internet, με την καταβολή των αντίστοιχων ποσών συνδρομής και ΤΑΠΕΤ .
* Οι Νομαρχιακές Αυτοδιοικήσεις, οι Δήμοι, οι Κοινότητες ως και οι επιχειρήσεις αυτών πληρώνουν το μισό χρηματικό ποσό της συνδρομής και ολόκληρο το ποσό υπέρ του ΤΑΠΕΤ.
* Η συνδρομή ισχύει για ένα ημερολογιακό έτος. Δεν εγγράφονται συνδρομητές για μικρότερο χρονικό διάστημα.
* Η εγγραφή ή ανανέωση της συνδρομής πραγματοποιείται το αργότερο μέχρι την 31ην Δεκεμβρίου κάθε έτους.
* Αντίγραφα διπλοτύπων, ταχυδρομικές επιταγές και χρηματικά γραμμάτια δεν γίνονται δεκτά.

Πληροφορίες Α.Ε. - Ε.Π.Ε. και λοιπών Φ.Ε.Κ.: 210 527 9000
Φωτοαντίγραφα παλαιών ΦΕΚ - ΒΙΒΛΙΟΘΗΚΗ - ΜΑΡΝΗ 8 - Τηλ. (210)8220885 - 8222924
Δωρεάν διάθεση τεύχους Προκηρύξεων ΑΣΕΠ αποκλειστικά από Μάρνη 8 & Περιφερειακά Γραφεία
Δωρεάν ανάγνωση δημοσιευμάτων τεύχους Α΄ από την ιστοσελίδα του Εθνικού Τυπογραφείου

Οι υπηρεσίες εξυπηρέτησης των πολιτών λειτουργούν καθημερινά από 08.00΄ έως 13.00΄



ΑΠΟ ΤΟ ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ
ΚΑΠΟΔΙΣΤΡΙΟΥ 34 * ΑΘΗΝΑ 104 32 * ΤΗΛ. 210 52 79 000 * FAX 210 52 21 004
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΕΥΘΥΝΣΗ: http://www.et.gr – e-mail: webmaster@et.gr